EUROPEAN COMMISSION

CASE DMA.100209 – SP – ALPHABET – ARTICLE 6(11)

(Only the English text is authentic)

Digital Markets Act

Regulation (EU) 2022/1925 of the European Parliament and of the Council

Article 8(2) Regulation (EU) 2022/1925

Date: 16/07/2026

This text is made available for information purposes only. A summary of this decision is published in all EU languages in the Official Journal of the European Union.

Parts of this text have been edited to ensure that confidential information is not disclosed. Those parts are replaced by a non-confidential summary in square brackets or are shown as […].

EUROPEAN
COMMISSION

Brussels, 16.7.2026
C(2026) 5091 final

COMMISSION IMPLEMENTING DECISION

of 16.7.2026

pursuant to Article 8(2) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector

Case DMA.100209 – SP – Alphabet – Article 6(11)

(Only the English text is authentic)

TABLE OF CONTENTS

1. Background to these specification proceedings 6
1.1. Introduction 6
1.2. Alphabet's proposal for compliance with Article 6(11) of Regulation (EU) 2022/1925 7
1.3. The importance of sharing anonymised ranking, query, click and view data with third party providers of online search engines on fair, reasonable, and non-discriminatory terms 9
1.4. Use of specification proceedings 11
2. Procedure 12
2.1. Legal framework for specification proceedings 12
2.2. Chronology of the current Proceedings 13
2.2.1. Event prior to the opening of the Proceedings 13
2.2.2. Events between the opening of Proceedings and Preliminary Findings 13
2.2.3. Preliminary Findings and access to file 14
2.2.4. The Public Consultation 14
2.2.5. Events following the Preliminary Findings and the Public Consultation 16
2.3. The Commission's investigation and engagement with Alphabet 18
2.3.1. The Commission's engagement with Alphabet 18
2.3.2. The Commission's investigation and engagement with third parties 27
3. The scope of Article 6(11) of Regulation (EU) 2022/1925 34
4. Measures that the Commission is specifying in this decision 36
4.1. Overview 36
4.2. Measures relating to eligibility of data beneficiaries 36
4.2.1. Introduction 36
4.2.2. Measures 37
4.2.3. The gatekeeper's view 39
4.2.4. The Commission's assessment 40
4.3. Measures relating to data scope and conditions of sharing 55
4.3.1. Parity principle 55
4.3.1.1. Introduction 55
4.3.1.2. The gatekeeper's view 56
4.3.1.3. The Commission's assessment 56
4.3.2. Data scope 62
4.3.2.1. Query data 62
4.3.2.2. View data 79
4.3.2.3. Click data 101

4.3.2.4. Ranking data 121
4.3.3. Conditions of data sharing 128
4.3.3.1. Invalid traffic 128
4.3.3.2. Latency, batches and time stamps 132
4.3.3.3. Method of sharing 140
4.3.3.4. Duration 144
4.3.3.5. Search session data 148
4.4. Measures relating to anonymisation 150
4.4.1. Legal framework 150
4.4.2. Alphabet's approach 153
4.4.2.1. Anonymisation measures 153
4.4.2.2. Contractual terms 155
4.4.2.3. Impact on the data shared 156
4.4.3. The gatekeeper's view 161
4.4.4. Measures 165
4.4.4.1. Technical measures 166
4.4.4.2. Contractual measures 219
4.4.5. Conclusions 266
4.5. Measures relating to the FRAND pricing of Alphabet's Search Data 266
4.5.1. Introduction 266
4.5.1.1. Alphabet's approach and pricing offer 267
4.5.1.2. The views of market participants 271
4.5.2. Measures 273
4.5.3. The Commission's assessment 277
4.5.3.1. FRAND under Article 6(11) of Regulation (EU) 2022/1925 277
4.5.3.2. Justifying a cost-based approach to FRAND pricing measures under Article 6(11) of Regulation (EU) 2022/1925 280
4.5.3.3. Operationalizing Alphabet's cost-based pricing measures under Article 6(11) of Regulation (EU) 2022/1925 287
4.5.3.4. Limitations to Alphabet's cost-based pricing measures under Article 6(11) of Regulation (EU) 2022/1925 293
4.6. Measures relating to process for Search Data acquisition and pre-acquisition data testing 294
4.6.1. Introduction 294
4.6.2. The gatekeeper's view 295
4.6.3. Process and practical arrangements for pre-acquisition technical testing 297
4.6.3.1. Introduction 297

4.6.3.2. Measures 298
4.6.3.3. The Commission's assessment 299
4.6.4. Process for finalising the Search Dataset 303
4.6.4.1. Introduction 303
4.6.4.2. Measures 303
4.6.4.3. The Commission's assessment 303
4.6.5. Process for finalising the licence agreements for the Search Dataset and the test data samples 305
4.6.5.1. Introduction 305
4.6.5.2. Measures 305
4.6.5.3. The Commission's assessment 305
4.6.6. Processes for making the Search Dataset available, reviewing eligibility of undertakings applying for eligibility, finalising pricing terms and ensuring continuity of access 306
4.6.6.1. Process for providing Search Dataset(s) and reviewing eligibility of undertakings applying for eligibility 306
4.6.6.2. Process for finalising pricing terms 309
4.6.6.3. Submission of Level 2 assurance reports to maintain access to the Search Dataset 311
4.6.6.4. Prior notification of a change of control and submission of Level 1 reasonable assurance reports to ensure continuity of access following a change of control of the third-party OSE 315
4.6.6.5. Submission of Level 2 reasonable assurance reports to ensure continuity of access following the commencement of insolvency proceedings 316
4.6.7. Processes for refusing, suspending and terminating access to the Search Dataset .. 318
4.6.7.1. Refusal decisions 318
4.6.7.2. Suspension of access 319
4.6.7.3. Termination following suspension 322
4.6.7.4. Expedited termination 325
4.6.8. Requirement to impose financial penalties in exceptional circumstances 327
4.6.8.1. Introduction 327
4.6.8.2. Measures 327
4.6.8.3. The Commission's assessment 328
4.6.9. Requirement to amend documents and obligation to inform the Commission, data protection supervisory authorities and the public of decisions granting, refusing, suspending, restoring or terminating access 330
4.6.9.1. Introduction 330
4.6.9.2. Measures 330
4.6.9.3. The Commission's assessment 331
5. Proportionality 333

6. Conclusion..... 338

COMMISSION IMPLEMENTING DECISION

of 16.7.2026

pursuant to Article 8(2) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector

Case DMA.100209 – SP – Alphabet – Article 6(11)

(Only the English text is authentic)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/1925 of the European Parliament and of the Council of 17 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act),[1] and in particular Article 8 thereof,

After consulting the Digital Markets Advisory Committee[2],

Whereas:

1. BACKGROUND TO THESE SPECIFICATION PROCEEDINGS

1.1. Introduction

(1) On 5 September 2023, the Commission adopted a decision designating Alphabet as a gatekeeper under Article 3(4) of Regulation (EU) 2022/1925 ("**Designation Decision**").[3] The Designation Decision lists the following core platform services ("**CPS**") that Alphabet provides and which individually constitute an important gateway for business users to reach end users: (i) its online intermediation service Google Shopping; (ii) its online intermediation service Google Play; (iii) its online intermediation service Google Maps; (iv) its online search engine ("**OSE**") Google Search; (v) its video-sharing platform service YouTube; (vi) its operating system Google Android; (vii) its web browser Google Chrome; and (viii) its online advertising services.

(2) Under Article 3(10) of Regulation (EU) 2022/1925, since 7 March 2024, Alphabet has been required to comply with the obligations laid down in *inter alia* Article 6(11) of Regulation (EU) 2022/1925 in relation to the CPSs listed in the Designation Decision, notably in relation to its OSE Google Search.

(3) Pursuant to Article 8(1) of Regulation (EU) 2022/1925, gatekeepers must ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of the Regulation. Gatekeepers must also ensure that the measures they implement are effective in achieving the objectives of the Regulation and of the relevant obligation.

---

1 OJ L 265, 12.10.2022, pages 1-66.

2 The opinion of the Digital Markets Advisory Committee can be found on the Commission's Comitology Register under meeting code CMTD(2026)1165: https://ec.europa.eu/transparency/comitology-register/screen/committees/C114400.

3 Decision C(2023) 6101 final.

(4) Pursuant to Article 8(2) of Regulation (EU) 2022/1925, the Commission may, on its own initiative or at the request of a gatekeeper, specify measures that the gatekeeper should implement to effectively comply with certain obligations. Article 6(11) of Regulation (EU) 2022/1925 is an obligation that is susceptible of being further specified.

1.2. Alphabet's proposal for compliance with Article 6(11) of Regulation (EU) 2022/1925

(5) According to Alphabet's most recent compliance report under Article 11 of Regulation (EU) 2022/1925, submitted on 6 March 2026 ("**Alphabet Compliance Report**"), Alphabet considers that it has ensured compliance with Article 6(11) of the Regulation with the launch of the European Search Dataset Licensing Program on 6 March 2024.[4] Under this programme, third-party OSEs can apply for access to a dataset containing anonymised ranking, query, click and view data ("**Google Search Data**"). The programme has been in operation since then with only limited modifications.[5]

(6) The dataset contains fields for the following: query string, country, device type (desktop or mobile/tablet, where Google's anonymisation protocols allow this to be broken out), query count, result (exact Uniform Resource Locator ("**URL**") for blue links, or type for other results, e.g., top text ad block or knowledge panel), average rank, impression count, and click count.[6] The dataset does not include paid results (i.e., ads), URLs in embedded results, user interaction data other than clicks (e.g., hover time) and location data.[7]

(7) Alphabet releases the Google Search Data quarterly, with a lag of one quarter.[8] The data for each quarter is therefore 4.5 months old on average. Alphabet provides the dataset in JSON format that is downloadable via Google Cloud. The dataset size is approximately 1.5 TiB per quarter and comprises around 30 billion rows for the entire European Economic Area ("**EEA**").[9] Beneficiaries can choose to procure the entire EEA dataset, or datasets for individual countries. Beneficiaries can also procure a 10% or 50% sample of each dataset.[10] Alphabet provides data to third parties for a maximum of three years.[11]

(8) Alphabet anonymises ranking, query, click and view data for the release of Google Search Data by applying two frequency thresholds:

(a) *k threshold:* Alphabet only includes queries that have been issued by at least 30 signed-in users globally over the past 13 months. Queries that pass this threshold are included on an allow list for a duration of five years.[12]

(b) *m threshold:* Results data such as average rank, impression count and click count are only provided for results viewed by at least five signed-in users in a given country and for a given device type during the quarter covered by the

---

4 Alphabet Compliance Report, Google Search Chapter, paragraph 93.

5 Modifications include data set pricing, the availability of a one-off fractional sample, and some changes to the anonymisation process.

6 Alphabet Compliance Report, Google Search Chapter, paragraph 97.

7 Beyond country-level, which is implied as the data is provided on a country-by-country basis.

8 Alphabet Compliance Report, Google Search Chapter, paragraph 99.

9 Alphabet Compliance Report, Google Search Chapter, paragraph 102.

10 Alphabet Compliance Report, Google Search Chapter, paragraph 101.

11 Alphabet Compliance Report, Google Search Chapter, paragraph 117(f).

12 Alphabet Compliance Report, Google Search Chapter, paragraph 106.

dataset. Data may be provided at a higher level of aggregation, e.g., without breakdown for device type.[13]

(9) As a result of those thresholds, Alphabet's anonymisation measures remove approximately [90-100]% of unique queries and [30-40]% of query volume from the dataset.[14]

(10) Alphabet has implemented a pricing scheme for the dataset which takes into account the following benchmarks: the pricing of scrapers which provide data on search result impressions, the pricing of search query data offered by ComScore, and the pricing of Microsoft's syndication offering.[15] Under the resulting pricing scheme, Alphabet charges a fixed fee per thousand queries, meaning that the price depends on the size of the dataset procured. The fee per thousand queries also varies between EUR 1.50 and EUR 9 depending on the beneficiary's revenue, resulting in an indicative price for the full EEA quarterly dataset between EUR 1.6 million and EUR 9.9 million.[16]

(11) Beneficiaries that wish to procure datasets under Alphabet's European Search Dataset Licensing Program must enter into a contract with Alphabet. Alphabet imposes the following main conditions on applicants:[17]

(a) Applicants must operate an OSE as defined in Article 2(6) of Regulation (EU) 2022/1925.

(b) Applicants must have a record of safeguarding user data to a high standard.

(c) Applicants must be financially viable.

(d) Applicants must not be directly or indirectly under the operation or control of a non-EEA State actor.

(e) Applicants must not operate a search engine optimisation ("**SEO**") business.

(12) Alphabet's template contract for the European Search Dataset Licensing Program includes several non-price terms for access to the dataset, including (i) a purpose of use restriction limited to optimising an OSE directed at users in the EEA; (ii) data security requirements such as measures for storing and processing the data, access controls and oversight; (iii) prohibition on re-identification; (iv) a one-year maximum data retention duration; and (v) restriction on third-party sharing of the data.[18]

(13) So far, [number of applicants] applicants have requested access to the dataset. Out of those, one applicant has received a licence for the dataset. The applicant that has received a licence for the dataset has so far acquired [a small sample of the dataset].[19]

---

13 Alphabet Compliance Report, Google Search Chapter, paragraph 107.

14 Alphabet's reply to RFI 2 of 22 December 2023, Doc ID 102-1, question 1c. Unique queries means the proportion of all distinct queries (all counted once) omitted. Query volume means share of all queries omitted, even if they are duplicates.

15 Alphabet Compliance Report, Google Search Chapter, paragraph 109. Syndication is the distribution of search results or paid advertisements from a primary search engine through another search engine or third-party website.

16 Alphabet Compliance Report, Google Search Chapter, paragraphs 110-116.

17 Alphabet Compliance Report, Google Search Chapter, paragraph 120.

18 Alphabet Compliance Report, Google Search Chapter, paragraph 117.

19 Alphabet Compliance Report, Google Search Chapter, paragraph 136 and Alphabet's reply to RFI 10 of 12 November 2025, Doc ID 637-1, question 18.

1.3. The importance of sharing anonymised ranking, query, click and view data with third party providers of online search engines on fair, reasonable, and non-discriminatory terms

(14) The quality of an OSE, and thereby the value it offers to end users and business users, increases as the number of users increases. Operators of OSEs store data on what end users searched for, what results the OSE provided in response to those searches, and how end users interacted with these results. Operators of OSEs use this data to improve their services, offering more relevant results in response to user queries.[20]

(15) Access to such ranking, query, click and view data poses a considerable barrier to entry and expansion for challenger OSEs. Google Search is by far the largest OSE globally and in the EEA. It has an estimated market share of around 90% globally, with the second largest player, Microsoft Bing, representing around 5%.[21] This means that Google Search has far more scale than any other OSE, and therefore gathers far more ranking, query, click and view data which enable it to optimise its OSE services.

(16) Google Search's advantage extends to the emerging AI search landscape, where users increasingly rely on AI chatbots to navigate the web. While AI chatbots, such as ChatGPT, Mistral Vibe or Claude boast innovative large language models ("**LLMs**") that generate original content, Alphabet's chatbots surpass them in searching and retrieving web content, thanks to the vast ranking, query, click, and view data accumulated from Google Search. This optimisation of OSE component of Alphabet's AI chatbots gives them a significant edge. By contrast, the AI search sector's contestability is hindered by barriers to entry and expansion, including substantial investment costs that are difficult to recoup and limited access to crucial inputs, such as search data. As AI chatbots with OSE functionalities compete with Gemini and AI Overviews on dimensions which are characterised with such barriers - web-scale indexing and retrieval, result relevance, ranking, and freshness - the risk grows that the underlying sectors will become dysfunctional or fail to operate effectively, ultimately undermining the ability of AI chatbot providers to optimise their OSE services at scale.[22]

(17) Due to their lack of scale, most challenger OSEs, be it traditional OSEs or AI chatbots with OSE functionalities, are at least in part dependent on syndication agreements or similar agreements where they access third-party search APIs. This means that they provide their users' queries to another OSE acting as their partner and display the partner's results on their OSE.

(18) The ranking, query, click and view Google Search data can be used to optimise OSE services in different ways. Some important use cases for this data include, but are not limited to:

(a) **Web crawling and index building:** OSEs rely on an index of documents that can be searched efficiently and be presented in response to a user query. An index is built by crawling the web using an automated bot called a web

---

20 Recital 61 of Regulation (EU) 2022/1925.

21 See Statcounter GlobalStats, https://gs.statcounter.com/search-engine-market-share, Doc ID 1732, last accessed on 19 February 2026.

22 E.g., https://www.pymnts.com/cpi-posts/ai-transforms-search-in-a-way-that-could-make-googles-default-advantage-stronger/?utm_source=Sailthru&utm_medium=email&utm_campaign=Main%20NL%2004/06&utm_term=daily_nl, Doc ID 1958, last accessed on 13 April 2026

crawler. Due to the size of the web, crawling and indexing the web is costly and strongly favours first movers.[23] Alphabet incurs significant costs annually to crawl the web and maintain its index.[24] Alphabet's advantage is further solidified because several major webpage owners restrict access to a select few crawlers to preserve bandwidth. Nearly all websites allow Google Search's crawler, as websites cannot afford to disappear from Google Search's index.[25] Many websites also proactively inform Google Search of website changes. Data provided under Article 6(11) of Regulation (EU) 2022/1925 can help challenger OSEs to focus their crawling strategy and manage their crawling budget. The data allows beneficiaries to analyse which URLs are frequently presented in search results and clicked on by users, yet are missing from the beneficiary's index. The data can also help OSEs to discover new websites that should be crawled and added to the index.

(b) **Refining retrieval and ranking systems:** OSEs continuously refine their retrieval and ranking systems to present end users with the most relevant results in response to a query. Ranking, query, click and view data provide insight in what end users search for and which results they interacted with. These past user interactions are used to improve the OSE's ranking and present the most relevant results to the end user. Ranking, query, click and view data is particularly valuable for low-frequency (or "**long-tail**") queries. Smaller OSEs are less likely to see these rare queries, meaning that they have insufficient data to present relevant results in response to them.[26]

(c) **SERP optimisation systems:** Search data also helps OSEs to determine the SERP layout and the display of search results to the end users.[27] Such data helps OSEs decide whether and when to present specialised results modules, such as knowledge panels or direct answers. It also helps structure the SERP and place specific URLs in dedicated parts of SERP, as either organic or advanced search results. Further, it is important for the visual appeal of SERP, deciding about the display of tabs, carousels, and rich results, such as image and video results.

(d) **Query analysis and spell checking, auto-suggestion and auto-completion:** OSEs analyse end user queries to understand user intent and to assist end users in formulating their queries by providing spell checking and spelling suggestions for queries that are likely to be misspellings, suggestions for related queries, and auto-completion of queries while the user is formulating the query. These services improve the end user experience of the OSE.

---

23 Investigation Of Competition In Digital Markets Majority: Staff Report And Recommendations (19 July 2022), House Committee on the Judiciary, Doc ID 1734, page 63.

24 See, for example, Commission Decision C(2017) 4444 in case AT.39740 Google Search (Shopping): "*Bing and Google each spend hundreds of millions of dollars a year crawling and indexing the deep Web. It costs so much that even big companies like Yahoo and Ask are giving up general crawling and indexing.*"

25 Investigation Of Competition In Digital Markets Majority: Staff Report And Recommendations (19 July 2022), House Committee on the Judiciary, Doc ID 1734, page 63.

26 See, for example, Roadblocks to Competition: Investigate Google's Non-Compliance with the EU's Digital Markets Act, available on https://spreadprivacy.com/investigate-google-dma/, Doc ID 1731, last accessed on 19 February 2026 and Investigation Of Competition In Digital Markets Majority: Staff Report And Recommendations (19 July 2022), House Committee on the Judiciary, Doc ID 1734, page 64.

27 See, for example, Search Engine Results Page (SERP) available at https://www.techtarget.com/whatis/definition/search-engine-results-page-SERP?utm_source=chatgpt.com, last accessed on 9 June 2026.

Ranking, query, click and view data can help an OSE to develop spell checking, autosuggestion and autocompletion. For instance, if a specific query is frequently followed by a second similar query, and the end user did not engage with any of the results displayed in response to the first query, that suggests that the second query could be a helpful autosuggestion. The data can also help OSEs with disambiguation (e.g., determining whether the query "jaguar" refers to an animal or a car brand).

(19) Gatekeepers operating OSEs as designated CPSs should therefore make available anonymised ranking, query, click and view data to allow challenger OSEs to surmount the scale gap and improve contestability in OSE services. Such data should be provided under fair, reasonable and non-discriminatory ("**FRAND**") conditions, so that challenger OSEs can afford the data and also to ensure that the provision of data does not itself confer disproportionate advantages on the gatekeeper.[28] When providing the data, the gatekeeper must anonymise end users' personal data for OSEs. However, the anonymisation measures employed must not substantially degrade the quality or usefulness of the data, as that would prevent challenger OSEs to use the data for the use cases outlined in recital (18).

(20) Increased contestability in OSE services benefits both end users and business users. Business users benefit from fairness and contestability in OSE services, as a greater choice of credible alternative OSE providers may increase contestability and fairness in relation to both free and paid ranking and search results (i.e., ads). This means that business users have additional sources of relevant organic web traffic and enjoy a more competitive marketplace for the placement of search ads.

(21) End users equally benefit since access to ranking, query, click and view data improves the search results of challenger OSEs, making them credible alternatives to Google Search. This increases choice and innovation in OSE services to the benefit of end users. For instance, challenger OSEs could offer services that are differentiated from Google Search, such as through a privacy-focused model,[29] supporting societal causes (e.g., environmental protection),[30] or AI integration (e.g., a chat interface that allows the user to search the web in a conversational way).

1.4. Use of specification proceedings

(22) While the obligation to grant third-party OSEs access to anonymised ranking, query, click and view data on FRAND terms is clearly set out in Article 6(11) of Regulation (EU) 2022/1925, gatekeepers may need guidance as to how to implement it. Such guidance may include aspects such as the identification of eligible beneficiaries, the scope of the data falling under the obligation and the modalities of sharing it, the exact steps required to achieve anonymisation and the methodology to ensure FRAND pricing.

(23) Recital 65 of Regulation (EU) 2022/1925 states that the Commission, following a dialogue with the gatekeeper concerned and after enabling third parties to make comments, may decide to further specify some of the measures that the gatekeeper concerned should adopt in order to effectively comply with obligations that are susceptible of being further specified or, in the event of circumvention, with all obligations.

---

28 See Article 8(8) of Regulation (EU) 2022/1925.

29 E.g., Qwant: https://betterweb.qwant.com/en/.

30 E.g., Ecosia: https://www.ecosia.org/.

(24) Pursuant to Article 8(7) of Regulation (EU) 2022/1925, in specifying the measures that the gatekeeper concerned is to implement in order to effectively comply with its obligations, the Commission shall ensure that the measures are effective in achieving the objectives of that Regulation and the relevant obligation and proportionate in the specific circumstances of the gatekeeper and the relevant service.

(25) Article 8(8) of Regulation (EU) 2022/1925 states that for the purposes of specifying the obligations under Article 6(11) of that Regulation, the Commission must assess whether the intended or implemented measures ensure that there is no remaining imbalance of rights and obligations on business users and that the measures do not confer an advantage on the gatekeeper which is disproportionate to the service provided by the gatekeeper to business users.

(26) The Commission is concerned that the current offer by Alphabet is not effective in achieving the objectives of Article 6(11) of Regulation (EU) 2022/1925. These concerns are supported by the almost absent take-up of the dataset offered by Alphabet despite significant interest by third-party OSEs.

(27) Therefore, to swiftly allow effective access of third-party OSEs to anonymised ranking, query, click and view data on FRAND terms, the Commission considers it appropriate to specify the measures that Alphabet should adopt to effectively comply with Article 6(11) of Regulation (EU) 2022/1925.

2. PROCEDURE

2.1. Legal framework for specification proceedings

(28) To specify the measures pursuant to Article 8(2) of Regulation (EU) 2022/1925, the Commission shall adopt an implementing act. This implementing act shall be adopted within six months from the opening of the proceedings pursuant to Article 20 of Regulation (EU) 2022/1925. Before adopting such an implementing act, the Commission shall communicate to the gatekeeper its preliminary findings, including the measures it is considering taking, within three months.

(29) Pursuant to Article 8(6) of Regulation (EU) 2022/1925, to effectively enable interested third parties to provide comments, the Commission shall, when communicating its preliminary findings to the gatekeeper or as soon as possible thereafter, publish a non-confidential summary of the case and the measures that it is considering taking or that it considers the gatekeeper concerned should take. The Commission shall specify a reasonable timeframe within which such comments are to be provided.

(30) Pursuant to Article 8(4) of Regulation (EU) 2022/1925 specification proceedings are without prejudice to the powers of the Commission to adopt a decision establishing non-compliance with any of the obligations laid down in Regulation (EU) 2022/1925 by a gatekeeper, including the possibility to impose fines or periodic penalty payments.

(31) Pursuant to Article 8(9) of Regulation (EU) 2022/1925, the Commission may, upon request or on its own initiative, decide to reopen specification proceedings where (i) there has been a material change in any of the facts on which the decision was based, (ii) the decision was based on incomplete, incorrect or misleading information, or (iii) the measures as specified in the decision are not effective.

2.2. Chronology of the current Proceedings

2.2.1. Event prior to the opening of the Proceedings

(32) Between March 2024 and January 2026, the Commission has frequently engaged with Alphabet on its compliance with Article 6(11) of Regulation (EU) 2022/1925. The Commission met Alphabet to discuss its compliance with Article 6(11) of Regulation (EU) 2022/1925 on multiple occasions,[31] and organised two compliance workshops with Alphabet, during which Alphabet's compliance with Article 6(11) of Regulation (EU) 2022/1925 was discussed.[32] The Commission sent to Alphabet 12 requests for information ("**RFIs**") in relation to Article 6(11) of Regulation (EU) 2022/1925.[33] The exchanges and discussions between the Commission and Alphabet covered issues such as the data scope, eligibility of beneficiaries, the terms of access and Alphabet's anonymisation approach.

(33) During the same period, the Commission has also frequently engaged with third parties on Alphabet's proposal concerning its compliance with Article 6(11) of Regulation (EU) 2022/1925, through meetings, calls, workshops and RFIs. The Commission has engaged with more than 20 third parties.

(34) On 26 January 2026 the Commission informed Alphabet of its intention to assist Alphabet in its compliance efforts in relation to Article 6(11) through opening of specification proceedings pursuant to Article 8(2) of Regulation (EU) 2022/1925.

2.2.2. Events between the opening of Proceedings and Preliminary Findings

(35) On 27 January 2026, the Commission adopted a decision opening proceedings under Article 20(1) of Regulation (EU) 2022/1925 with a view to the adoption of a decision under Article 8(2) of that Regulation specifying the measures that Alphabet must implement regarding its OSE Google Search to effectively comply with Article 6(11) of that Regulation (the "**Proceedings**").[34]

(36) On 5 February 2026, the Commission held a state of play meeting with Alphabet in which it outlined the preliminary scope of the specification proceedings and summarised the proposed engagement between the Commission and Alphabet during the Proceedings.

(37) Between opening on 27 January 2026 and communication of the preliminary findings on 16 April 2026, the Commission held five meetings with Alphabet, to discuss topics within the scope of the Proceedings.[35]

(38) Between opening on 27 January 2026 and communication of the preliminary findings on 16 April, the Commission issued 11 RFIs to Alphabet.[36]

---

31 Including on 18 September 2024, 11 December 2024, 10 January 2025, and 11 November 2025.

32 The Commission organised compliance workshops with Alphabet on 21 March 2024 and 1 July 2025 during which Alphabet's compliance with Article 6(11) of Regulation (EU) 2022/1925 was discussed.

33 Requests for information of 28 November 2023 (Doc ID […]), 22 December 2023 (Doc ID […]), 28 February 2024 (Doc ID […]), 15 May 2024 (Doc ID […]), 22 July 2024 (Doc ID […]), 13 March 2025 (Doc ID […]), 26 March 2025 (Doc ID […]), 10 September 2025 (two requests) (Doc ID […]), 12 November 2025 (two requests) (Doc ID […]), and 13 November 2025 (Doc ID […]).

34 Decision C(2026) 582 final (the "**Opening Decision**").

35 Meetings of: 5 February 2026 (state of play); 11 February 2026 (on contractual terms of data sharing); 12 February 2026 (on fair, reasonable and non-discriminatory terms); 2 March 2026 (on search technical infrastructure and data), and 3 March 2026 (on anonymisation).

36 Requests for information of 28 January 2026 (Doc ID […]), 30 January 2026 (Doc ID […]), 11 February 2026 (two requests) (Doc ID […]), 12 February 2026 (Doc ID […]), 13 February 2026 (Doc ID […]), 18 February 2026 (Doc ID […]), 19 February 2026 (Doc ID […]), 6 March 2026 (Doc ID […]), 23 March 2026 (Doc ID […]) and 27 March 2026 (Doc ID […]).

(39) Between 27 January 2026 and 16 April 2026, the Commission continued its investigation and engagement with third parties, through meetings, calls RFIs and review of third-party submissions.

(40) On 10 April 2026, prior to the adoption of its preliminary findings, the Commission held with Alphabet a courtesy state-of-play conference call during which the Commission outlined the scope of the preliminary findings.

2.2.3. Preliminary Findings and access to file

(41) On 16 April 2026, 11 days ahead of the three months legal deadline set out in Article 8(5) of Regulation (EU) 2022/1925, the Commission communicated its preliminary findings to Alphabet pursuant to Articles 8(5) and 34(1) of Regulation (EU) 2022/1925 (the "**Preliminary Findings**"), providing Alphabet with the opportunity to comment on its findings and the proposed measures ("**Preliminary Measures**") by 1 May 2026.

(42) On 17 April 2026, the Commission received Alphabet's request to access the Commission's file pursuant to Articles 8(2) and 8(3) of the Commission Implementing Regulation (EU) 2023/814. On that same day and in reply to Alphabet's request, the Commission provided Alphabet with all documents used in the Preliminary Findings pursuant to Article 8(2) of the Commission Implementing Regulation (EU) 2023/814. In addition, on the same day, the Commission adopted a decision setting out the terms of disclosure for the purpose of access to the Commission's file pursuant to Article 34(4) of Regulation (EU) 2022/1925 and Article 8 of Regulation (EU) 2023/814 (the "**Terms of Disclosure decision**").[37]

(43) On the working-day following Alphabet's request, i.e. 20 April 2026, the Commission afforded Alphabet's external legal counsel access to the case file in a data room pursuant to Article 8(3) of the Commission Implementing Regulation (EU) 2023/814. Access to the data room was provided from 20 April until 24 April 2026. On 23 April 2026 Alphabet requested to extend the data room access for an additional day, i.e. 27 April 2026 and the Commission agreed.[38] However, the data room report prepared in the context of the data room and provided by Alphabet's external legal counsel to the Commission (in the data room) on 27 April 2026 did not comply with the data room rules annexed to the Commission's Terms of Disclosure decision, and the data room remained open until 30 April 2026, when Alphabet's external legal counsel finalised the confidential and non-confidential versions of the data room report. The non-confidential version of the data room report was shared with Alphabet on 30 April 2026.[39]

2.2.4. The Public Consultation

(44) On 16 April 2026, and in line with Article 8(6) of Regulation (EU) 2022/1925, the Commission published a non-confidential summary of the case and the proposed measures to enable interested third parties to provide their comments on the proposed measures ("**the Public Consultation**").

(45) The Public Consultation was open until 1 May 2026. The Commission received over 140 contributions from third parties, end users and other interested third parties. All

37 Decision C(2026) 2685

38 Email exchange of 23 April 20206, Doc ID […].

39 Doc […].

submissions were shared with Alphabet on a rolling basis, as previously communicated to Alphabet's external legal counsel in the call of 15 April 2026.[40]

(46) During the Public Consultation and shortly after it, the Commission held several calls with third parties who reached out to it in the context of the public consultation.[41] Minutes of these calls and any additional submissions from third parties were shared with Alphabet on a rolling basis.[42]

(47) Following the opening of the Public Consultation,[43] Alphabet has reached out, through emails, calls and meetings, to over 60 third parties, including academics in the privacy field, think tanks, advertisers, publishers, consumer and industry associations.[44] Alphabet shared its criticism on the Preliminary Measures with the addressees of its outreach and asked them to take part in the public consultation. Some addressees were asked to help Alphabet spread its views by sharing them with others.[45] Alphabet shared with these third parties various position papers and pamphlets criticising different aspects of the Preliminary Measures. Alphabet's outreach materials were tailored around at least three campaigns, concerning privacy risks,[46] advertisers' concerns[47] and publishers' concerns.[48] In addition Alphabet disseminated a general paper named "*DMA search data sharing input"* comprising one paragraph views on each section of the Public Consultation.[49] Following Alphabet's outreach, some of the addressees shared with Alphabet their draft submission for review and comments prior to submitting it in the Public Consultation,[50] or the final submission.[51] At least 30 addressees of Alphabet's

---

40 The Commission sent third parties' contributions to Alphabet by email on 29 April 2026 (Doc ID […]), 30 April 2026 (Doc ID […]), 5 May 2026 (Doc ID […]), and 6 May 2026 (Doc ID […]).

41 Calls of 24 April 2026, 29 April 2026 (two calls), 4 May 2026, 18 May 2026, 20 May 2026, 8 June 2026 and 10 June 2026.

42 The Commission sent the minutes, submissions and substantive email correspondence with third parties on 13 May 2026 (Doc ID […]), 31 May 2026 (Doc ID […]), 2 June 2026 (Doc ID […]), 9 June 2026 (Doc ID […]), 24 June 2026 (Doc ID […]), 8 July 2026 and 13 July 2026.

43 Alphabet's engagement with some of the third parties in relation to the Proceedings started before the public consultation. See, for example, Alphabet's reply to RFI 14, Annexes Q1.01 (Doc ID […]) and Q1.06 (Doc ID […]).

44 Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.0 Doc ID […]; Alphabet's reply to RFI 18 of 5 June 2026, Annex Q1.1, Doc ID […].

45 See Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.53 (Doc ID […]),

46 See (i) Alphabet's one pager pamphlet titled "*Digital Markets Act 6(11) Privacy Concerns*", sent to at least 15 addressees, see for example Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.09 (Doc ID […]), and Index of annexes, Doc ID […]; (ii) Alphabet's "*Position Paper on 6(11) Anonymisation*", sent to at least 10 addresses, see for example Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.12 (Doc ID […]), and Index of annexes, Doc ID […]; In addition, Alphabet sent several template emails focused on the matter of privacy and anonymisation, see, for example, Alphabet's reply to RFI 14 of 19 May 2026, Annexes Q2.03 (Doc ID […]) and Q2.80 (Doc ID […]), each sent to a number of addressees.

47 See Alphabet's one pager pamphlet titled "*Digital Markets Act 6(11) Advertiser Concerns*", sent to at least 10 addressees, see, for example, Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.16 (Doc ID […]), and Index of annexes, Doc ID […].

48 See Alphabet's reply to RFI 14 of 19 May 2026, Annexes Q2.02 (Doc ID […]), Q2.04 (Doc ID […]), Q2.53 (Doc ID […]).

49 See, for example, Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.01 (Doc ID […]), sent to at least 12 addressees, see Alphabet's reply to RFI 14 of 19 May, Index of annexes (Doc ID 2509-5).

50 See, for example: Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.27 (Doc ID […]); Annex Q2.78 (Doc ID […]); Annex Q2.66 (Doc ID […]), where, in response to the draft submission Alphabet notes: "*I had our Europe legal team review the paper and they confirmed everything is good and accurate*", and Annexes Q2.45 (Doc ID […]) and Q2.75 (Doc ID […]), where it appears Alphabet proposed revisions to the third parties' draft submissions.

outreach made a submission in response to the Public Consultation.[52] At least 18 respondents to the Public Consultation, which were included in Alphabet's outreach, also have, or have had, a relationship with Alphabet within the last two years, including membership, affiliation, sponsorship, funding, research affiliation and employment. Alphabet has also confirmed that several respondents were remunerated by Alphabet for their participation in the Public Consultation.[53]

2.2.5. Events following the Preliminary Findings and the Public Consultation

(48) On 21 April 2026, Alphabet requested an extension of the deadline to respond to the Preliminary Findings. On 23 April 2026, the Commission granted an extension until Friday, 15 May 2026, thereby granting Alphabet a total of one calendar month to submit its observations.[54] On 11 May 2026, Alphabet requested an additional extension until the end of Sunday, 17 May 2026. On the same day, the Commission granted the extension.[55]

(49) On 18 May 2026, Alphabet provided its response to the Preliminary Findings ("**Alphabet's response to the Preliminary Findings**").[56]

(50) On 19 May 2026 Alphabet submitted a letter setting out an alternative anonymization approach for the Commission's consideration.[57]

(51) On 6, 7, 13 and 22 May 2026 the Commission held meetings with Alphabet to discuss Alphabet's feedback on the measures, during which Alphabet presented slide decks.[58]

(52) On 26 May 2026, the Commission held a tripartite meeting with Alphabet, [market participant], [market participant], [market participant], and [market participant]. The meeting was followed by additional submissions by [market participant] on 2 June 2026, by Alphabet on 4 June 2026,[59] and a joint submission of [names of market participants] on 9 June 2026. The Commission has shared the additional submissions by these third parties with Alphabet quicky after receival.[60]

(53) On 27 May 2026 Alphabet sent a letter to the Commission asking to carve out anonymisation measures from the current Proceedings, to allow sufficient time for analysis and testing,[61] on 29 May 2026 the Commission confirmed it will consider Alphabet's request together with Alphabet's other comments on the Preliminary measures.[62]

---

51 See, for example Alphabet's reply to RFI 14 of 19 May 2026, Annexes Q2.52-53 (Doc ID […]); Q2.90-91(Doc ID […]).

52 Alphabet's reply to RFI 14 of 19 May 2026, Annex 2.0, Doc ID […]; Alphabet's reply to RFI 18 of 5 June 2026, Annex Q1.01, Doc ID […].

53 Alphabet's reply to question 2(b) of RFI 14 of 19 May 2026, paragraph 20, Doc ID […]; Alphabet's reply to question 5(b) of RFI 18 of 5 June 2026, paragraph 13, Doc ID […].

54 Doc ID […].

55 Doc ID […].

56 Alphabet's response to the Preliminary Findings, Doc ID [...].

57 Doc ID 2429. A version for third parties was shared on 21 May 2026, Doc ID […].

58 Slides of 6 May 2026 on anonymisation (Doc ID […]); Slides of 7 May 2026 on frequency (Doc ID […]), Slides of 13 May 2026 on contractual measures (Doc ID […]), and slides of 22 May 2026 on anonymisation (Doc ID […]).

59 Doc ID […].

60 Emails of 2 June 2026, Doc ID […], and 9 June 2026, Doc ID […].

61 Doc ID […].

62 Doc ID […].

(54) On 4 June, Alphabet submitted a note proposing revisions to the preliminary contractual measures.[63]

(55) After the communication of the preliminary findings on 16 April, the Commission issued 9 additional RFIs to Alphabet.[64]

(56) By way of courtesy, the Commission shared revised measures ("**Draft Revised Measures**") with Alphabet on 8 June 2026, as well as a report on testing by external experts, commissioned by the Commission.[65] On 10 June 2026, the Commission shared with Alphabet underlying code information in relation to the report on testing.[66] The Commission granted Alphabet until 15 June 2026 to submit its observations and offering a meeting to provide any clarification.[67] In response to Alphabet's extension request until 22 June 2026, the Commission granted a two days extension until 17 June 2026 in relation to the report on testing only to account for the sharing of the underlying code information and ensure that Alphabet has a full week to submit comments having received all relevant information.

(57) On 10 June, upon Alphabet's request, a State of Play meeting was held where the Commission presented the revisions to the preliminary measures and the reasons for them and Alphabet had the opportunity to comment on the Draft Revised Measures. Following up on this, on 11 June 2026, Alphabet submitted a "*Proposal for alternative process for anonymization*".[68]

(58) On 15 June 2026, Alphabet submitted its observations on the revised measures ('**Alphabet's response to the Revised Measures**'),[69] together with an annex setting out suggested amendments to the Draft Revised Measures.[70] On 18 June 2026, Alphabet submitted its observations on the external expert report on testing that accompanied the Commission Draft Revised Measures.[71]

(59) On 2 July 2026, upon Alphabet's request, a meeting was held where the Commission explained why it does not consider it appropriate or required to revise the timeline or the process for the specification of the anonymisation measures. In addition, the Commission informed Alphabet of the main revisions to the measures it is considering. On 5 July 2026, the Commission replied to Alphabet's letters of 27 May 2026 and 11 June 2026, confirming its intention to specify the anonymisation measures as part of the Proceedings.

(60) On 3 July 2026, and on 7 July 2026, by way of courtesy, the Commission shared with Alphabet the draft final measures. On 6 July 2026, further to Alphabet's request and by way of courtesy, the Commission shared with Alphabet the envisaged clause referring to the future review of the measures.

---

63 Doc ID […].

64 Requests for information of 11 May 2026 (Doc ID […]), 12 May 2026 (Doc ID […]), 19 May 2026 (Doc ID […]), 20 May 2026 (Doc ID […]), 22 May 2026 (Doc ID […]), 28 May 2026 (Doc ID […]), 5 June 2026 (Doc ID […]), 12 June 2026 (Doc ID […]) and 17 June 2026 (Doc ID […]).

65 Doc ID […].

66 Doc ID […].

67 Doc ID […]

68 Doc ID […].

69 Alphabet's response to the Revised Measures, Doc ID […].

70 Doc ID […]

71 Doc ID […].

2.3. The Commission's investigation and engagement with Alphabet

(61) Alphabet claims that the Commission did not conduct a genuine, open-minded, and independent investigation;[72] that in its Preliminary Findings, the Commission uncritically and disproportionately adopted the views of self-interested third parties and did not seek views of other relevant market participants;[73] that the public consultation on the Preliminary Measures was not fair and objective;[74] and that the Commission failed to engage in a genuine dialogue with Alphabet prior to the adoption of its Preliminary Findings.[75] Alphabet further submits that it was not granted proper access to the Commission's file.[76] In the subsequent sections, the Commission addresses these claims.

2.3.1. The Commission's engagement with Alphabet

(62) Against the background of the regulatory dialogue with Alphabet concerning the implementation of Alphabet's obligations under Article 6(11) of Regulation (EU) 2022/1925, which has been ongoing since the designation of Alphabet's OSE Google Search, on 5 September 2023, the Commission conducted the specification proceedings in a diligent and transparent manner, taking account of the framework of Regulation (EU) 2022/1925 and in line with the principle of good administration.

(63) **First,** as described in section 2.2 of this Decision and below, the Commission actively engaged with Alphabet in a genuine and open dialogue prior to and throughout the proceedings, contrary to Alphabet's claims that the Commission failed to engage in a genuine dialogue prior to the Preliminary Findings.[77]

(64) ***In the first place***, the Commission carried out a regulatory dialogue with Alphabet since the entry of its obligation to comply with Article 6(11) of Regulation (EU) 2022/1925 into force in March 2024, discussing Alphabet's compliance proposal and various alternative compliance measures. As early as 12 December 2023, during a high-level meeting with Alphabet concerning its compliance with Regulation (EU) 2022/1925, the Commission expressed its view that, based on feedback from third parties, Alphabet's compliance proposal requires improvement. On 18 September 2024, during a meeting with Alphabet, the Commission repeated its view that Alphabet's compliance proposal in relation to Article 6(11) of the Regulation requires significant improvement. The Commission expressed its doubts concerning Alphabet's anonymisation method that resulted in little or no useful data being available to beneficiaries; the level of aggregation, which reduced the dataset utility; the fact that the dataset excluded relevant paid and advanced search results; the lag of data sharing, which appeared to be too long and the commercial terms which made the offer unattractive. In November 2025, more than two months ahead of the formal opening of the Proceedings, and following other meetings on matters within the scope of these Proceedings, the Commission held a comprehensive meeting with Alphabet and presented its preliminary views on several matters within the scope of these Proceedings. Alphabet was made aware of the upcoming formal opening of the proceedings ahead of the decision opening Proceedings.

---

72 Alphabet's response to the Preliminary Findings, paragraph 602, Doc ID [...], and Alphabet's Data Room Report, section II, Annex 4 to Alphabet's response to the Preliminary Findings, Doc ID […].

73 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 603-609.

74 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 610-612.

75 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 613-616.

76 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 617-622.

77 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 613-616.

(65) ***In the second place***, further to the opening of the Proceedings, the Commission guided Alphabet through the list of its concerns during the state-of-play meeting of 5 February 2026, informing Alphabet in detail about the scope of the specification proceedings. On 19 February 2026, further to a request by Alphabet, the Commission provided Alphabet with a high-level outline of the envisaged anonymisation measures and listed some of the elements that were being explored by the Commission.[78] The Commission continued its engagement with Alphabet on all matters within the scope of the Proceedings in a series of meetings prior to the adoption of the Preliminary Findings, on 11 February 2026, 12 February 2026, 2 March 2026, and 3 March 2026. During these meetings Alphabet presented slide decks explaining its views on matters within the scope of the Proceedings.[79] The Commission also gave Alphabet a read-out of the then envisaged preliminary anonymisation measures as well as an outline of the remaining preliminary measures on 10 April 2026. The Commission notes that it has granted all meetings requested by Alphabet.

(66) ***In the third place,*** further to these meetings and the topics discussed in them, Alphabet made two submissions to the Commission. A legal opinion on the "*[i]nterplay between the Anonymization Requirement under Article 6(11) of the DMA and the GDPR*" was submitted on 7 April 2026,[80] and a paper titled "*Art. 6(11) does not require Google to support GenAI grounding*" was submitted on 14 April 2026.[81]

(67) ***In the fourth place***, the Commission issued 23 RFIs to Alphabet to inform its views and assessment ahead of the issuance of the Preliminary Findings. Twelve RFIs were sent prior to the opening of the Proceedings, and additional eleven RFIs were sent since the opening of Proceedings until the Preliminary Findings. The Commission notes that Alphabet has frequently provided delayed and incomplete replies to the Commission's requests and did not always facilitate the Commission's analysis and investigation. For example, in order to understand and assess Alphabet's anonymisation approach, on 26 March 2025, the Commission issued RFI 6 to Alphabet, in which the Commission requested Alphabet to provide it with access to a representative one-week sample of (Irish) Google Search data and accompanying statistics about the dataset. Alphabet eventually granted effective access to the data requested in RFI 6 only on 1 July 2025, and to the statistics only on 13 July 2025.[82] After receiving access and resolving the operational issues, the Commission found inconsistencies in the dataset provided by Alphabet and, on 23 July 2025, requested Alphabet to explain them. Further to numerous exchanges and acknowledgement by Alphabet of the inconsistencies,[83] on 12 September 2025 Alphabet provided access to a new dataset, and re-submitted corrected dataset statistics in its reply to RFI 6 on

---

78 Doc ID […]

79 Doc ID […] (slides presented on 12 February 2026), Doc ID […] (Slides presented on 2 March 2026), and Doc ID […](Slides presented on 3 March 2026). During the meeting of 11 February 2026 no slides were presented.

80 Doc ID […]

81 Doc ID […]

82 Following deadline extension requests, Alphabet provided the data in two tranches (on 28 May 2025 and on 20 June 2025), however the Commission encountered numerous issues related to accessing and working on the dataset. See email exchanges between the Commission and Alphabet on RFI 6 dated 26 March 2025 to 22 May 2025 (Doc ID […]); 28 May 2025 to 10 June 2025 (Doc ID […]); 28 May 2025 to 1 July 2026 (Doc ID […]); 28 May 2025 to 13 July (Doc ID […]), and 28 May 2025 to 15 July (Doc ID […]).

83 See email exchanges of 23 July 2025 to 12 August 2025 (Doc ID […]).

11 November 2025.[84] On 19 November 2025 the Commission identified further inconsistencies in the newly shared statistics, but those were not addressed by Alphabet, despite being informed.[85]

(68) ***In the fifth place,*** the specification procedure foreseen in Article 8(5) of Regulation (EU) 2022/1925 requires the Commission to explain the measures it considers taking *in the preliminary findings*, which should be communicated to the gatekeeper within three month from the opening of proceedings: "*With a view of adopting the decision under paragraph 2, the Commission shall communicate its preliminary findings to the gatekeeper within 3 months from the opening of the proceedings under Article 20. In the preliminary findings, the Commission shall explain the measures that it is considering taking or that it considers the gatekeeper concerned should take in order to effectively address the preliminary findings.*" Alphabet's claim that the Commission did not discuss with it the measures before adopting its preliminary findings, "*losing 3 months – half of the total duration of the proceedings*",[86] goes beyond the requirements of Article 8(5) of the Regulation. In any case, as demonstrated in previous recitals, the Commission did extensively engage with Alphabet on all matters within the scope of the Proceedings. In particular, in relation to the anonymisation measures,[87] as mentioned, the Commission raised its concerns in relation to Alphabet's anonymisation approach prior to the opening of proceedings; third parties' comments stating similar concerns were shared with Alphabet; after the opening of Proceedings, the Commission provided Alphabet with a high-level outline of the envisaged anonymisation measures and listed some of the elements that were being explored by the Commission; RFI questions addressed to Alphabet demonstrated the various query thresholding and metadata generalisation that were explored by the Commission.[88] Indeed, as a result of the Commission's extensive engagement with Alphabet on the matter of anonymisation, Alphabet was able to provide its views and comments on the anonymisation methods that were being explored by the Commission, as demonstrated by Alphabet's slide deck presented during the technical meeting of 3 March 2026 on anonymisation.[89]

(69) ***In the sixth place*****,** in order to allow more time to discuss the preliminary measures with Alphabet and third parties, the Commission communicated its preliminary findings in the current case 11 days ahead of the three months legal deadline set out in Article 8(5) of Regulation (EU) 2022/1925.

(70) ***In the seventh place,*** as described in section 2.2 of this Decision, the Commission continued the engagement with Alphabet after the adoption of the Preliminary Findings. In particular, the Commission: (i) held five meetings with Alphabet to discuss Alphabet's feedback on the measures;[90] (ii) moderated a tripartite meeting between Alphabet and potential beneficiaries to discuss the anonymisation

---

84 See email exchanges of 23 July 2025 to 9 October 2025 (Doc ID […]) and of 4 to 11 November 2025 (Doc ID […]).

85 See Commission's email to Alphabet of 19 November 2025, Doc ID […].

86 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 613.

87 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 613

88 See for example, questions 9, 11, 14 and 15 of RFI dated 12 November 2025 (Doc ID […]); questions 1,2, 6-9 of RFI dated 11 February 2026 (Doc ID […]); questions 1,2 6 and 7 of RFI dated 28 January 2026 (Doc ID […]), and question 3 of RFI dated 13 February 2026 (Doc ID […]).

89 See for example slides 13-19 of the presentation (Doc ID […]), which refer to identifier detection filters, word frequency thresholding, and metadata thresholding, all relating to technical anonymisation measures that the Commission was exploring.

90 Meetings of 6, 7, 13 and 22 May 2026 and of 10 June 2026.

measures;[91] (iii) issued seven additional RFIs to follow-up on claims made by Alphabet in meetings with the Commission and in its response to the Preliminary Findings;[92] and (iv) carefully reviewed and assessed Alphabet's response to the Preliminary Findings[93] and submissions by Alphabet, which Alphabet sent to the Commission after the deadline to reply to the Preliminary Findings.[94]

(71) ***In the eighth place***, for the sake of completeness, the Commission sent all submissions of third parties to the Public Consultation to Alphabet on a rolling basis, as well as all minutes of meetings with third parties that took place after the adoption of the Preliminary Findings, irrespective of whether these documents are used in this Decision.

(72) ***In the ninth place***, in the spirit of good cooperation, the Commission sent the Draft Revised Measures to Alphabet on 8 June 2026 granting Alphabet an additional opportunity to comment on the Commission's Draft Revised Measures. Following this, the Commission engaged further with Alphabet on its views and comments on the Draft Revised Measures during a meeting on 10 June 2026 and through the review of written comments submitted by Alphabet on 11, 15 and 18 June 2026. The Commission also sent an expert report to Alphabet on 8 June 2026 setting out the results of testing conducted to evaluate the technical measures concerning anonymisation and potential improvements to these measures. Access to the data underlying the report was granted on 10 June 2026.

(73) ***In the tenth place***, as part of the Commission's genuine and open engagement with Alphabet, the Commission assessed Alphabet's views, and used this assessment, where considered appropriate, as input for designing the measures in the Annex to this Decision. Several revisions to the Preliminary Measures address comments provided by Alphabet. Examples include the introduction of latency to the sharing of data; the exclusion of ads' URLs from the dataset and the introduction of an *ad hoc* audit process.

(74) ***In the eleventh place*****,** pursuant to the process measures specified in the Annex to this Decision, Alphabet has 45 days as of the date of notification of this Decision to prepare an application form for the Search Dataset.[95] This will be reviewed and monitored by the Commission following the adoption of the Decision in the context of the Commission's duties pursuant to Article 26(1) of Regulation (EU) 2022/1925, thus allowing more time and further consideration of elements concerning the implementation of the measures.

(75) In light of the above and taking into account the extent of the Commission's engagement with Alphabet as set out in this section and in section 2.2 of this Decision, the Commission considers that it discharged its duties under Article 41 of the Charter of Fundamental Rights of the EU (right to good administration). The Commission also duly considered the principle of proportionality, Alphabet's fundamental rights and Alphabet's intellectual property rights as set out in sections 3, 4.3.1 and 5 of this Decision.

---

91 Meeting of 26 May 2026.

92 Requests for information of 11 May 2026 (Doc ID […]), 12 May 2026 (Doc ID […]), 20 May 2026 (Doc ID […]), 22 May 2026 (Doc ID […]), 28 May 2026 (Doc ID […]), 12 June 2026 (Doc ID […]) and 17 June 2026 (Doc ID […]).

93 Doc ID [...], and annexes doc IDs […].

94 Submission of 19 May 2026, Doc ID […]; 4 June 2026 (two submissions) Doc ID […]; 27 May 2026, Doc ID […]; 11 June 2026, Doc ID […]; 15 June 2026, Doc […], and annex Doc ID […], and 18 June 2026, Doc ID […].

95 As defined in the Annex.

(76) **Second**, the Commission does not consider that the timeline and process for the specification of measures concerning anonymisation should be revised or that the measures concerning anonymisation should be carved out of these Proceedings as requested by Alphabet.[96]

(77) ***In the first place,*** it is for the Commission to determine the scope of a specification and the required level of detail. The Commission's decision to open the Proceedings has clearly identified anonymisation as one of the areas in Alphabet's European Search Dataset Licensing Program that would benefit from the specification of measures to ensure that Alphabet's compliance is effective in achieving the objective of Article 6(11) of Regulation (EU) 2022/1925.[97] As explained in the Opening Decision, Alphabet's anonymisation approach removes [90-100]% of unique queries and [30-40]% of query volume from the dataset, and third parties state that this significantly degrades the usefulness of the data and that there are alternative anonymisation methods available that result in significantly less degradation.[98] Prior to the opening of the Proceedings, Alphabet has been unwilling to consider alternative anonymisation methods, despite comments addressed to it by third parties[99] and concerns raised by the Commission.[100]

(78) ***In the second place,*** Article 8 of Regulation (EU) 2022/1925 sets out a clear process for specification proceedings which ensures that draft measures can be improved through input from the gatekeeper and stakeholders. To allow the Gatekeeper to provide its comments, Article 8(5) of the Regulation sets that "*the Commission shall communicate its preliminary findings to the gatekeeper within 3 months from the opening of the proceedings*". To effectively enable interested third parties to provide comments, Article 8(6) of the Regulation dictates that upon the communication of the preliminary findings to the gatekeeper the Commission must "*publish a non-confidential summary of the case and the measures that it is considering taking or that it considers the gatekeeper concerned should take*", specifying "*a reasonable timeframe within which such comments are to be provided*". As detailed in section 2.2, the Commission has strictly followed the procedure set out in Article 8 of the Regulation.

(79) Pursuant to Article 8(2) of Regulation (EU) 2022/1925, the specification decision "*shall be adopted within 6 months from the opening of proceedings*". The Article does not provide for an exception to the 6-months timeline. This means that at the

---

96 In its letter of 27 May 2026 (Doc ID […]), Alphabet argues that the preliminary measures are flawed but that "there is now insufficient time left to develop genuinely robust anonymization measures". Alphabet suggest that the development of the correct anonymization measures should be carved out from the ongoing specification process, which, according to Alphabet, could be done either by the Commission refraining from specifying the anonymization measures under the current procedure, or by specifying only the general principles of the anonymization measures at a high level that provides flexibility in developing the details. In its letter of 11 June 2026 (Doc ID […]), Alphabet repeats it proposal to specify only substantive principles that will apply to anonymization and proposes to dedicate 60 days to develop anonymisation measures with the support of an advisory privacy panel to be established by the Commission, and additional 30 days for testing by independent technical experts to be appointed by the Commission. Alphabet suggests that if the Commission then evaluates that the measures can proceed, "*the Commission can render* [the measures] *binding by re-opening proceedings pursuant to Art. 8(9) DMA and adopting them in form of specifications*."

97 Opening Decision, paragraph 14(a).

98 Opening Decision, paragraph 14(a).

99 See: Third party emails to Alphabet, of 5 December 2023 (Doc ID […]) and of 17 Jan 2024 (Doc ID […]). In addition, during a compliance workshop of 1 July 2025, stakeholders noted that the dataset offered by Alphabet to comply with Article 6(11) of the Regulation still require some work, in particular in relation to the anonymisation method.

100 Meetings of 12 December 2023 and 18 September 2024.

end of the 6-months timeline, the Commission should adopt a specification decision setting out measures based on the facts that it has collected. Contrary to Alphabet's proposal in its letter of 11 June 2026, the Commission cannot use Article 8(9) of the Regulation as a mean to prolongate the 6-months timeline and take more time to assess the facts that it has collected during the specification procedure. Article 8(9) of the Regulation sets out a limited set of circumstances in which the Commission can re-open proceedings. This includes the possibility to re-open where there has been a material change in any of the facts on which the decision was based. This possibility must however concern new facts and cannot be conflated with the possibility to take more time to assess the fact that have been collected within the 6-month timeframe set in Article 8 of the Regulation. Alphabet's proposed use of Article 8(9) of the Regulation would therefore constitute an abuse of the process set in Article 8 of the Regulation and would go against the legislator's intention to conclude the specification proceedings within six months.

(80) ***In the third place***, the Proceedings effectively allowed for very detailed engagement, by the Commission, Alphabet, and third parties, on anonymisation. **Firstly,** a large share of the Commission's open and genuine engagement with Alphabet throughout these proceedings, was devoted to discussing and assessing the anonymisation requirement in Article 6(11) of Regulation (EU) 2022/1925. At least 17 RFIs sent to Alphabet prior to or during these Proceedings included questions concerning anonymisation.[101] Anonymisation and anonymisation related issues were discussed in detail during at least seven meetings,[102] and Alphabet made several submissions concerning anonymisation to the Commission.[103] **Secondly,** the preliminary anonymisation measures were subject to extensive testing by Alphabet and the Commission. As explained in section 4.4 of this Decision, Alphabet conducted its own testing during a period of at least 1.5 months. As also described in section 4.4 of this Decision, the Commission has conducted its own testing and analysis of the anonymisation measures. **Finally,** third parties have provided their comments on the preliminary anonymisation measures in reply to the Public Consultation. The measures specified in the Annex to this Decision reflect the Commission's careful assessment of all the input collected throughout the Proceedings, and considers that they comply with the anonymisation requirement in Article 6(11) of the Regulation.

(81) ***In the fourth place***, already the measures communicated to Alphabet in the Preliminary Findings reflected significant engagement of the Commission, Alphabet

---

101 RFIs of 28 November 2023 (Doc ID […]), 22 December 2023 (Doc ID […]), 28 February 2024 (Doc ID […]), 15 May 2024 (Doc ID […]), 22 July 2024 (Doc ID […]), 26 March 2025 (Doc ID […]), 12 November 2025 (Doc ID […]), 28 January 2026 (Doc ID […]), 11 February 2026 (Doc ID […]), 13 February 2026 (Doc ID […]), 27 March 2026 (Doc ID […]), 11 May 2026 (Doc ID […]), 20 May 2026 (Doc ID […]), 22 May 2026 (Doc ID […]), 28 May 2026 (Doc ID […]), 12 June 2026 (Doc ID […]) and 17 June 2026 (Doc ID 2598).

102 Meetings of 11 December 2024 (Meeting at Alphabet's request to discuss a report commissioned by Alphabet on the anonymisation of the search dataset); 11 February 2026 (contractual terms of data sharing); 2 March 2026 (search technical infrastructure and data), 3 March 2026 (anonymisation), 6 May 2026 (anonymisation), 13 May 2026 (contractual measures), and 22 May 2026 (Alphabet's alternative anonymisation proposal). In addition, a large number of calls and exchanges between the Commission and Alphabet were devoted to arranging access to the Commission and its contracted experts to a representative sample of the dataset, in order to allow the Commission to understand and assess Alphabet's anonymisation approach.

103 See, for example: Submission of 21 November 2024 "Privacy Expert Report on DMA Art.6(11) Google Search Data Sharing" (Doc ID […]); Submission of 28 November 2024 titled "Expert Opinion: The Anonymization Requirement under Article 6(11) of the DMA in the context of the GDPR", Doc ID […]; "updated expert opinion on the legal concept of anonymization", dated 25 March 2026, Doc ID […], and "Alternative anonymization approach" dated 18 May 2026, Doc ID 2429-2.

and third parties in relation to anonymisation, which took place before and after the opening of Proceedings. Third parties provided their views on Alphabet's anonymisation approach already in 2023,[104] and continued to provide various their views on anonymisation to the Commission until the adoption of the Preliminary Findings through submissions,[105] RFI replies,[106] and meetings.[107] The Commission has expressed its concerns in relation to Alphabet's anonymisation approach as early as 12 December 2023, and has requested Alphabet with access to search data to conduct its own analysis of Alphabet's anonymisation approach already on 26 March 2025.[108] Questions concerning anonymisation were included in at least 11 RFIs sent to Alphabet prior to the Preliminary Findings.[109] Acknowledging the Commission's concerns in relation to the anonymisation measure applied by Alphabet, already on 21 November 2024, Alphabet has shared with the Commission a technical expert report it commissioned, analysing its anonymisation approach.[110] On 28 November Alphabet made an additional submission concerning anonymisation.[111]

(82) ***In the fifth place***, further review of the measures and their effectiveness is ensured through Article 2 of this Decision, which establishes that "*the effectiveness and impact of these measures will be evaluated within two years following the adoption of this Decision, taking into account technological developments*". Article 8(9) of the Regulation also provides that the Commission can reopen proceedings where there has been a material change in any of the facts on which the decision was based.

(83) **Third**, the Commission followed strictly the procedure set out in the law in full respect of Alphabet's rights of defence, and Alphabet's right to access the Commission's file was respected.

(84) ***In the first place***, as described in section 2.2 above, in line with Article 34 of Regulation (EU) 2022/1925 and Articles 8(2) and 8(3) of the Commission Implementing Regulation (EU) 2023/814, Alphabet was granted access to the full Commission file. Alphabet was provided with all documents used in the Preliminary Findings on the same day the Commission received Alphabet's request to access the Commission's file. Alphabet was further given access, via its specified external

---

104 Third party emails to Alphabet, of 5 December 2023 (Doc ID […]) and of 17 Jan 2024 (Doc ID […]). Alphabet was given an opportunity to respond to those views, see Commission's RFI of 28 February 2024, Doc ID […]. In addition, during a compliance workshop of 1 July 2025, stakeholders noted that the dataset offered by Alphabet to comply with Article 6(11) of the Regulation still require some work, in particular in relation to the anonymisation method.

105 See, for example, [market participant]'s submissions on anonymisation dated June 2023, Doc ID […] and 9 September 2025, Doc ID […]; [market participant]'s, [market participant]'s and [market participant]'s submission dated 4 June 2024, Doc ID […]; [market participant]'s submission of 4 September 2025, Doc ID […].

106 See, for example, third party replies to Commission RFI 18 November 2025, Doc ID […]; Third party replies to Commission RFI of 12 February 2026, Doc ID […].

107 See, for example, minutes of meetings with third parties dated 30 September 2024, Doc ID […] February 2026, Doc ID […]; 26 November 2025, Doc ID […]; 21 February 2026, Doc ID […], 7 January 2026, Doc ID […]; 13 January 2026, Doc ID […], 22 January 2026, Doc ID […].

108 Commission's RFI of 26 March 2025, Doc ID […].

109 RFIs of 28 November 2023 (Doc ID […]), 22 December 2023 (Doc ID […]), 28 February 2024 (Doc ID […]), 15 May 2024 (Doc ID […]), 22 July 2024 (Doc ID […]), 26 March 2025 (Doc ID […]), 12 November 2025 (Doc ID […]), 28 January 2026 (Doc ID […]), 11 February 2026 (Doc ID […]), 13 February 2026 (Doc ID […]) and 27 March 2026 (Doc ID […]).

110 Alphabet's letter of 21 November 2024 (Doc ID […]) sending "Privacy Expert Report on DMA Art.6(11) Google Search Data Sharing" (Doc ID […]).

111 Submission of 28 November 2024 titled "Expert Opinion: The Anonymization Requirement under Article 6(11) of the DMA in the context of the GDPR", Doc ID […].

advisers,[112] to the case file in a data room on the working-day following Alphabet's request.

(85) ***In the second place,*** contrary to Alphabet's claims,[113] and as stated in the Commission's Terms of Disclosure decision,[114] Alphabet's right to access the Commission's file does not extend to the minutes of the Commission's meetings with the European Data Protection Board ("**EDPB**"). Therefore, the fact that Alphabet was not granted access to these minutes does not represent a breach of Alphabet's right of defence. The Commission notes that, already on 21 April 2026, Alphabet requested that the minutes of the Commission's meetings with the EDPB be made available to it. On 23 April 2026, the Commission denied Alphabet's request, referring to the Terms of Disclosure Decision and to Article 34(4) of Regulation (EU) 2022/1925 as the basis for its reply. On 27 April 2026 Alphabet repeated its request and on 19 May the Commission provided a second reply, explaining how the fourth and fifth sentences of Article 34(4) of Regulation (EU) 2022/1925 provide a legal basis for denying Alphabet access to the minutes of the meetings with EDPB. Indeed, as explained in the Commission's replies to Alphabet, pursuant to Article 34(4), fourth and fifth sentences, of Regulation (EU) 2022/1925, no access to the Commission's file is to be granted to confidential information and internal documents of the Commission or the competent authorities of the Member States, including correspondence between them. The EDPB is composed of the heads of the national data protection authorities of the Members of the European Economic Area, as well as the European Data Protection Supervisor tasked to ensure the consistent application of Regulation (EU) 2016/679. Accordingly, the EDPB is composed of competent authorities of Member States. Correspondence between the Commission and the EDPB, including the exchange of minutes and the minutes themselves, documenting oral exchanges during a meeting between the Commission and the EDPB, therefore falls, in principle, within the exception set out in Article 34(4), fourth sentence, of Regulation (EU) 2022/1925. For completeness, Article 34(4) of Regulation (EU) 2022/1925, fourth and fifth sentences do not require the Commission to conduct a balancing exercise between the necessity of safeguarding the rights of the defence and the interest in maintaining confidentiality. In any event, even if the Commission were to conduct a balancing test, the balance of interests weighs heavily against disclosure of the minutes of the Commission's meetings with the EDPB. This is because, the exchanges between the Commission and the EDPB, held in compliance with the principles of good administration and sincere cooperation, took place at technical level and must be regarded as internal, rather than a formal position of the Commission or the EDPB. While granting access to the minutes would undermine confidential internal deliberations between the Commission and the EDPB and internal deliberations of the EDPB, Alphabet does not need access to the EDPB Minutes to ascertain the EDPB's feedback on the Commission's Preliminary Findings. The EDPB's comments on the Commission's Preliminary Findings was provided in the EDPB's letter of 5 May 2026[115] to the Commission and was shared with Alphabet on 6 May 2026,[116] in full respect of Alphabet's right of defence.

---

112 As defined in the Commission's Terms of Disclosure decision.

113 Alphabet's response to the Preliminary Findings, paragraphs 617-620, Doc ID [...].

114 Recitals 24-26.

115 EDPB comments on the proposed measures of 5 May 2026, Doc ID […].

116 Email of 6 May 2026, Doc ID […].

(86) ***In the third place***, contrary to Alphabet's claims,[117] granting Alphabet access to documents in the Commission's file, beyond those quoted in the Preliminary Findings, only through its Specified External Advisers (and not to Alphabet directly) is compliant with the existing regulatory framework and did not violate Alphabet's right of defence. **Firstly,** Article 8(3) Regulation (EU) 2023/814 provides for access to the full file, including confidential and non-cited documents, to a limited number of specified external advisers, under strict terms of disclosure which are established in a Commission decision. This procedure ensures confidentiality while offering the gatekeeper access to the full file through its specified external advisers. Accordingly, as explained in section 2.2 above, the Commission adopted the Terms of Disclosure Decision, which specified the modalities for access in a data room setting, in accordance with Article 8(3)(e) of Commission Implementing Regulation (EU) 2023/814. Pursuant to the Terms of Disclosure Decision, Alphabet's specified external advisers were granted, at the Commission's premises, access to unredacted versions of all documents in the case file, only subject to the exceptions specified in the Terms of Disclosure Decision. **Secondly,** Regulation (EU) 2022/1925 establishes a distinct procedural framework from that applicable to antitrust cases. The Commission Implementing Regulation (EU) 2023/814 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 establishes a specific procedural framework for gatekeepers' access to file, tailored to the nature of the Regulation (EU) 2022/1925. This framework balances the need for efficient and timely investigations with the preservation of the gatekeeper's rights of defence. The General Court confirmed in its ByteDance judgment that Regulation (EU) 2022/1925 is characterised by a regulatory structure that differs from traditional competition law proceedings.[118] Therefore, Alphabet's reliance on antitrust case-law on access to the file are not relevant for the current case.[119]

(87) ***In the fourth place***, any inadvertent gaps in the Commission's case file were filled shortly after identification and the data room duration was extended. Therefore, contrary to its claims,[120] Alphabet was granted proper access to the Commission's file. Further to the opening of the data room, the Commission received questions from Alphabet's Specified External Advisers in the data room, flagging potential gaps in the Commission's case file. The Commission has immediately acted to identify the source of the issue and restore the integrity of the case file and Alphabet's access to it.[121] The Commission has identified a number of documents concerning Alphabet's compliance with Article 6(11) of Regulation (EU) 2022/1925, or Article 6(11) of the Regulation more generally, all pre-dating Alphabet's designation as a gatekeeper for Google Search and the entry into force of the obligations set in Article 6(11) of the Regulation and which were included in a separate case file. In addition, the Commission identified two documents which were not registered to the Commission's case file. The Commission has immediately retrieved the documents, registered them in the present case file and granted

---

117 Alphabet's response to the Preliminary Findings, paragraphs 621-622, Doc ID [...].

118 Judgment of the General Court of 17 July 2024, ByteDance Ltd v European Commission, Case T 1077/23, ECLI:EU:T:2024:478.

119 Alphabet refers to the cases of *Aalborg Portland*, *Qualcomm* and *Bulgarian Energy Holding*. See Alphabet's response to the Preliminary Findings, paragraph 622, Doc ID [...].

120 Alphabet's data room report, paragraphs 106-109, Annex 4 to Alphabet's response to the Preliminary Findings, Doc ID […].

121 The Commission has shared with Alphabet's Specified External Advisers in the data room two notes describing the methodology applied to export files to the Commission case file, dated 27 January 2026 (Doc ID […]), and 23 April 2026 (Doc ID […]).

Alphabet's Specified External Advisers access to all these documents in the data room on 22 April 2026.[122] While it is regrettable that some documents were unintentionally missing from the Commission's case file at the moment of opening the data room, this error was corrected upon identification, thus not causing any harm to Alphabet's right to defence. The data room duration was later extended, thus allowing Alphabet sufficient time to review and assess these documents.

(88) The Commission notes that the gap in the Commission's case file, which was immediately remedied and which did not cause harm to Alphabet's right to defence, was in fact much smaller than what is argued by Alphabet: (i) a large share of the documents that were added to the data room, i.e., 13 documents, of the 56 documents referred to by Alphabet as documents that were added to the data room on 22 and 23 April 2026,[123] did not fill any gap in the data room and were irrelevant to Alphabet's right to defence.[124] None of these documents contain substance relevant to the assessment of the case, and most of them concerned outreach to third parties informing them of the Public Consultation; (ii) 28 documents constitute non-substantial exchanges with third parties, such as outreach emails attaching Alphabet's compliance solution and requesting comments on it, requests for non-confidential versions of submissions and minutes, and other non-substantial documents. As such, their importance to Alphabet's right to defence is extremely limited; and (iii) six documents are duplicates, interim or non-confidential versions of documents already included in the data room upon its opening, meaning that Alphabet already had access to them. In addition, eight of the remaining documents concern third party submissions from 2022-2023, which are mostly short and unelaborated. As these parties remained in contact with the Commission, their later, and more elaborate submissions were part of the case file upon the opening of the data room. Finally, the addition of 15 documents to the data room on 24 April 2026,[125] was done as courtesy and not in order to fill in a gap in the case file. These 15 documents are print-screens of links in another document that was made accessible in the data room and were added to the data room for Alphabet's Specified External Advisers' convenience, as the data room is not connected to the internet.

(89) **In conclusion**, against these considerations, the Commission rejects Alphabet's procedural claims regarding the Commission's open and genuine engagement with it, the timeline for the specification of measures concerning anonymisation and Alphabet's right of defence and access to the Commission's file.

2.3.2. The Commission's investigation and engagement with third parties

(90) The Commission's investigation was diligent, fair and impartial and complied with the principles of good administration.

---

122 While Alphabet claims that access to one of these documents was granted only on 23 April 2026 (see paragraph 107 of the data room report, annex 4 to Alphabet's response to the Preliminary Findings), access to this document was granted together with other document already on 22 April 2026, in printed form. On 23 April 2026 access to the same document was granted in digital form.

123 Paragraph 107 of the data room report, annex 4 to Alphabet's response to the Preliminary Findings, Doc ID […].

124 These 13 documents were registered to the Commission's case file in the usual course of business after the opening of the data room and before the registration of the documents missing from the case file took place. As any addition of documents to the data room requires continuity from the last document shard in the data room, documents registered in the usual course of business were added to the data room together with the documents meant to remedy the identified gaps in the Commission's case file.

125 Paragraph 109 of the data room report, annex 4 to Alphabet's response to the Preliminary Findings Doc ID […].

(91) **First**, to inform its specification, the Commission sought views, expertise and technical input from a wide range of stakeholders, in an open and genuine manner.

(92) ***In the first place***, prior to and throughout the Proceedings, the Commission has sought views of and engaged with a variety of third parties, including OSE providers, academics in the field of privacy, consultancies in the fields of economics and audit, and other market participants. As described in section 2.2, the Commission sought third parties' views through meetings, calls, RFIs and invitations to provide views in writing. Both the existence of Article 6(11) of Regulation (EU)2022/1925 and the Opening Decision are public, and third parties were free to reach out to the Commission and provide their views, which the Commission reviewed and assessed as part of its investigation. Indeed, several third Parties reached out to the Commission on their own initiative to provide their views either before or after the Opening Decision.[126]

(93) ***In the second place*****,** the Commission was assisted by both in-house and external experts. As further explained in section 4.4.4.1 of this Decision, for the purpose of elaborating an alternative anonymisation method, the Commission has commissioned an expert report from a recognised expert in the field of anonymisation. The expert hired by the Commission participated in calls with Alphabet and with other market participants, had access to data from Alphabet and third parties as well as access to a sample of the dataset, thus allowing them to establish a view based on a complete and detailed review of the various interests related to the application of Article 6(11) of Regulation (EU) 2022/1925. The Commission has also commissioned two recognised experts in the field of anonymisation to conduct data testing. The Commission also relied on its own in-house expertise for the purpose of elaborating an alternative anonymisation method, and in particular that of the Chief Technology Officer in the Commission's Directorate-General for Competition.

(94) ***In the third place*****,** in line with Article 8(6) of Regulation (EU) 2022/1925, in order to "*effectively enable interested third parties to provide comments*", following the adoption of its Preliminary Findings, the Commission published a non-confidential summary of the case and the measures that it was considering and invited any interested party to express their view on the preliminary measures considered by the Commission in a Public Consultation. Article 8(6) of the Regulation was conceived by the legislator exactly for the purpose of ensuring transparency and open feedback from any interested third parties. Indeed, in response to the Public Consultation, the Commission received over 140 submissions from a wide range of stakeholders, including think tanks, academics, industry associations, OSE providers, competent authorities of Member States and individual citizens.

(95) ***In the fourth place*****,** the Commission engaged closely with the EDPB, the EU body composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor ("**EDPS"**), tasked to ensure the consistent application of Regulation (EU) 2016/679 in the Union.[127] The Commission discussed the preliminary measures to ensure anonymisation with the EDPB on 6 February

---

126 See, for example: Minutes of a meeting with an online business dated 26 May 2023, Doc ID […]; email to the Commission by a consultancy, dated 19 September 2023, Doc ID […]; Email to the Commission from an academic dated 19 March 2024, Doc ID […], and an email from a market participant dated 3 February 2026, Doc ID […].

127 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC ("Regulation (EU) 2016/679"), OJ L 119, 4.5.2016, section 3 "European Data Protection Board".

2026, 18 March 2026, and 30 March 2026, in order to inform the EDPB of the considered measures and to allow them to provide meaningful views in the context of the Public Consultation. The EDPB provided its comments on the proposed measures to ensure anonymisation on 5 May 2026. On 15 June 2026, the Commission presented and discussed the Draft Revised Measures with the EDPB.

(96) ***In the fifth place*****,** contrary to Alphabet's claims, seeking views of potential beneficiaries is desired and a sign of good administration. In its response to the Preliminary Findings, Alphabet criticises the "*Commission's approach of focusing disproportionately on views and requests from potential recipients*".[128] As explained in the preceding and subsequent recitals, the Commission sought views of a wide range of stakeholders, and in particular those of Alphabet, and has adequately assessed and considered them when designing the measures. However, the Commission also notes that it is necessary and appropriate to seek the views of potential beneficiaries of Alphabet's obligation pursuant to Article 6(11) of Regulation (EU) 2022/1925, and to give careful attention to their views. As providers of OSE services, potential beneficiaries are well placed to provide information on search data and search technologies. In addition, considering that Alphabet itself is likely to have conflicting interests when providing its views on the implementation of the Article, potential beneficiaries can bring complementary perspectives and assist the Commission to form its views by challenging Alphabet's submissions and offering alternatives. Furthermore, achieving the objectives of Article 6(11) of the Regulation is only feasible if eligible third party OSEs acquire the dataset from Alphabet. Views of potential recipients on how to improve the utility and therefore attractiveness of the dataset, while ensuring full compliance with the Article's requirements, are therefore of significant importance. In this respect, seeking views of providers of AI service providers who may potentially qualify as OSEs is equally justified. The Commission fails to see why the fact that, in order to encourage engagement by such market participants, the Commission titled its emails "*opportunities for AI providers*", demonstrates that the Commission "*failed to conduct a comprehensive investigation*" or any of the similar arguments made by Alphabet in that respect.[129]

(97) ***In the Sixth place*****,** while the commission invited a wide range of third parties to provide their views on Alphabet's compliance with Article 6(11) of Regulation (EU) 2022/1925, not all parties engaged with the Commission at the same level of intensity. The fact that some third parties engaged more actively with the Commission, while others did not, does not evidence flaws in the Commission's investigation.

(98) ***In the seventh place*****,** contrary to Alphabet's claims,[130] by testing specific views with market participants, or providing a framework for their reply, the Commission did not pre-assume the answers to its questions nor led the stakeholders to any specific answer. The questions Alphabet identified as allegedly leading,[131] appear to fall in

---

128 Alphabet's response to the Preliminary Findings, paragraph 609, Doc ID [...].

129 Alphabet's data room report, paragraphs 31-39, Annex 4 to Alphabet's response to the Preliminary Findings, Doc ID […].

130 Alphabet's response to the Preliminary Findings, paragraphs 610-611, Doc ID [...], and Alphabet's data room report, paragraphs 21-30, Annex 4 to Alphabet's response to the Preliminary Findings, Doc ID […].

131 For example (the questions are quoted in full and not partially as done by Alphabet): (i) How must Alphabet anonymise the data based on technical measures complemented by contractual measures, without unnecessarily degrading the quality and usefulness of the data?; (ii) View data: Would advanced search (e.g. direct answers, such as converted currency; knowledge panels, containing factual

one of the following types: (i) the Commission provided a framework in which a meaningful answer should be provided,[132] or (ii) tested a specific theory and sought stakeholders' views on it.[133] The questions did not steer respondents toward a specific answer, and did not imply a "correct" answer. By contrast, the questions addressed by the Commission to third parties in the Public Consultation and its various RFIs provided a neutral structure to guide respondents without influencing their actual opinions. By introducing a framework to the questions, the Commission sought to increase the chances of receiving meaningful replies, that would contribute to its assessment. Defining a framework to the reply, increased the questions' clarity and ensured respondents interpret the question consistently. Any guidance provided in the questions was provided to define clearly the matters on which the Commission was seeking views.

(99) For example, the question inviting respondents to the Public Consultation to provide views on the anonymisation measures provided guidance as to what effective anonymisation measures are required to achieve (i.e., anonymising the data based on technical measures complemented by contractual measures, without unnecessarily degrading the quality and usefulness of the data), and clarified (i) that the technical measures will be complemented by contractual measures, and (ii) that quality and usefulness of the data should not be degraded unnecessarily. This clarification relies on the language of recital 61 of Regulation (EU) 2022/1925, clarifying that a gatekeeper "*should ensure the protection of the personal data of end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data, without substantially degrading the quality or usefulness of the data*" and on the Joint EDPB and Commission guidelines on the interplay between DMA and GDPR, version for public consultation ("**Joint Guidelines**"),[134] stating that "*[w]hen selecting among various possible ways of achieving anonymisation of data of end users shared under Article 6(11) DMA, gatekeepers should select the one that preserves the most quality and usefulness of the data*"[135] and that "*anonymisation should be achieved by appropriate technical measures for alteration of the data, complemented by organisational, administrative and contractual measures to mitigate residual likelihood of identification*".[136] Absent this

---

information, or entity result blocks, identifying results for different individual entities) URL links help you optimise your online search engine services? If so, how?; Please provide concrete examples; (iii) Please explain whether and why data freshness is relevant to optimise your online search engine service; (iv) For each of the query data types listed in the table below: (a) Please indicate the relative importance for OSE services optimisation compared to other query data, by allocating 1 to the most important data field and succeeding numbers in descending order of importance to all data fields. (b) Please rank the importance of each type of information to OSE services optimisation from 1 to 5, where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. (c) Explain your answer and provide any other comments you may have. (d) If any type of query data which is important for OSE services optimisation is missing from the table, please add it to the table specifying its metrics and required granularity; (v) In […]'s view, does user interaction data which is not strictly measured by clicks, such as hover time, scrolling patterns and abandonments fall under click data category of article 6(11)? If so, please explain why and provide any supporting evidence (e.g., reference in industry reports or internal documents, etc.).

132 Questions (i) and (iv) in the previous footnote.

133 Questions (ii), (iii) and (v) in the previous footnote.

134 Joint EDPB and Commission guidelines on the interplay between DMA and GDPR, version for public consultation ("Joint Guidelines"), Doc ID […]. Said version of the Joint Guidelines is available at: https://digital-markets-act.ec.europa.eu/document/download/8ba0913f-2778-4a6d-9c58-10f8c7ead009_en?filename=Joint_COM-EDPB_GLS_interplay_DMA_GDPR_for_public_consultation.pdf

135 Join Guidelines, Doc ID 1880, paragraph 180

136 Join Guidelines, Doc ID 1880, paragraph 181

clarification (and as a matter of fact, even despite it) the Commission risked receiving submissions that ignore the legal framework, providing views that would therefore not contribute to the Commission's assessment. Similarly, when asking market participants to rate the importance of various data types to OSE optimisation, the Commission did not lead respondents to identify all data types as important. In fact, one of the options was to rate data types as "*1= not important*", and indeed respondents' ratings varied across data types. Also in questions where the Commission sought views on a specific point and asked whether respondents agree or disagree with a given approach, the Commission's questions did not imply a "correct" answer and anyway asked respondents to explain their views and provide examples, thus ensuring meaningful engagement and not just repetition of the allegedly sought after answer. In fact, as flagged by Alphabet, in some cases several respondents provided a negative reply, not validating the Commission's alleged views.[137]

(100) **Second,** the measures specified by the Commission reflect the Commission's independent assessment of all the input collected during its investigation.

(101) ***In the first place*****,** the main stakeholder with whom the Commission engaged is Alphabet, and not any third party. In particular, the number of RFIs addressed to and meetings held with Alphabet is incomparable to any of the third parties who provided their input to the Commission's investigation.

(102) ***In the second place*****,** views of both Alphabet and of third parties were appropriately considered and are reflected in this Decision and the specified measures as further demonstrated in section 4 of this Decision. As discussed in recital (73), several revisions to the preliminary measures address comments provided by Alphabet. The Commission has also carefully reviewed and considered all contributions received in response to the public consultation.[138] The Commission has given due consideration to all contributions and input it has received based on their merit and a factual analysis, and irrespective of whether contributions originated from organisations connected to Alphabet or of Alphabet's influencing campaign as described in recital (47).[139] Where appropriate, the measures specified in the present Decision reflect changes to the measures and clarifications that address public consultation input. For

---

137 For example, in relation to click data, a number of market participants disagreed with the definition tested by the Commission (see replies to RFI 1 of 28 January 2026 of [market participant], Doc ID […], question 3; [market participant], Doc ID […], question 8, and [market participant], Doc ID […], question 6.

138 The Commission notes that over 60 submissions made in response to the Public Consultation and which Alphabet identifies as criticising the Preliminary Measures, are very short, un-substantiated submissions of individuals in the Public Consultation. As explained in section 4.4.4.1, several of these submissions, which did not engage with the measures proposed in the Preliminary Findings, but object to the transfer of data altogether, or were under the impression that the Commission would gain access to search data, appear to have been made shortly after Alphabet announced that "*it took its security team less than two hours to reverse-engineer the European Commission's proposed search-data sharing rules and link individual queries back to named users, including matching some to sensitive details like pregnancy" (Politico Pro Fair Play newsletter of 27 April 2026)* and claimed that the measures put personal data at risk.

139 The suggestion by Alphabet that the Commission could disregard certain contributions that is has received ("*It would be troubling if the Commission were now to look for a pretext to disregard the outcome of its consultation and persist in a biased focus on a handful of complainants*", see, Alphabet's response to RFI 14 of 19 May 2026, paragraph 10, Doc ID [market participant]), is therefore unfounded and incorrect. While the Commission believes that it is important to be transparent on Alphabet's effort to influence the public consultation, this has no bearing on the systematic factual assessment that the Commission has conducted of all input it has received in order to improve the measures and provide additional explanation and justification on the rationale for these measures.

example, the measure concerning invalid traffic was revised to clarify that to the extent technically possible, Alphabet should apply the same methods and processes it applies itself to exclude invalid traffic, addressing concerns raised by third parties in response to the Public Consultation that invalid traffic can be used to over exclude useful search data. Similarly, in view of the public consultation and Alphabet's comments, under the measure concerning anonymisation, the metadata threshold has been increased, location and interaction data has been coarsened, mini-sessions are capped at three queries, ad URLs are removed, and the measures now provide transparency on the implementation of personal data detectors in the context of the entity threshold.

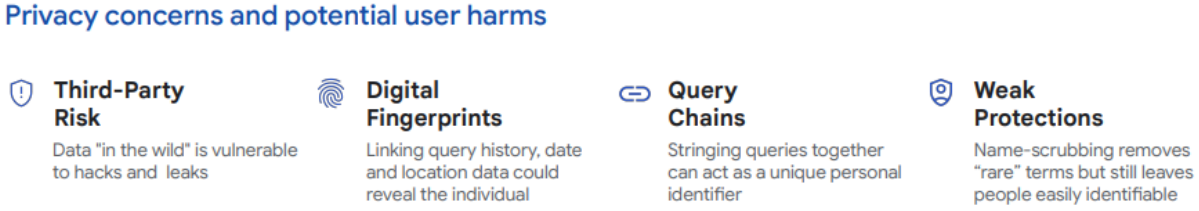
(103) **Third,** while this has no bearing on the factual analysis that the Commission has conducted of all contributions and input received, the Commission observes that Alphabet attempted influencing the views of respondents to the Public Consultation, through a widespread outreach in relation to the Commission's Preliminary Measures.

(104) ***In the first place***, as described in section 2.2 of this Decision, Alphabet conducted a well organised and widespread outreach in an attempt to encourage and influence submissions on the Commission's preliminary measures in the Public Consultation, reaching out to a wide range of stakeholders and asking them to submit their views in the Public Consultation.

(105) ***In the second place***, Alphabet provided to the addressees of its outreach a partial and biased representation of the Preliminary Findings. As mentioned in section 2.2, Alphabet shared with third parties various position papers and pamphlets criticising different aspects of the Preliminary Measures. These materials provided a partial, distorted and biased view of the Preliminary measures.

(106) For example, Alphabet shared with at least 15 stakeholders an infographic pamphlet titled "*Digital Markets Act 6(11) Privacy Concerns*".[140] While not providing any information on the regulatory context for the data sharing, the pamphlet states data will be released "*in the wild*", ignoring the fact that data will be released only to eligible OSEs who meet extensive contractual requirements that are verified through an audit process. The document further refers to the anonymisation measures as "*name scrubbing*", clearly understating and misrepresenting the measures (see Figure 1 below). It also provides a list of hypothetical examples of re-identification without any analysis against the draft measures and applicable legal test. A similar reference to data "*in the wild*" is repeated in a pamphlet titled "*Digital Markets Act 6(11) Advertisers Concerns*", sent to at least 10 stakeholders.[141]

Figure 1: Alphabet's pamphlet "Privacy Concerns":



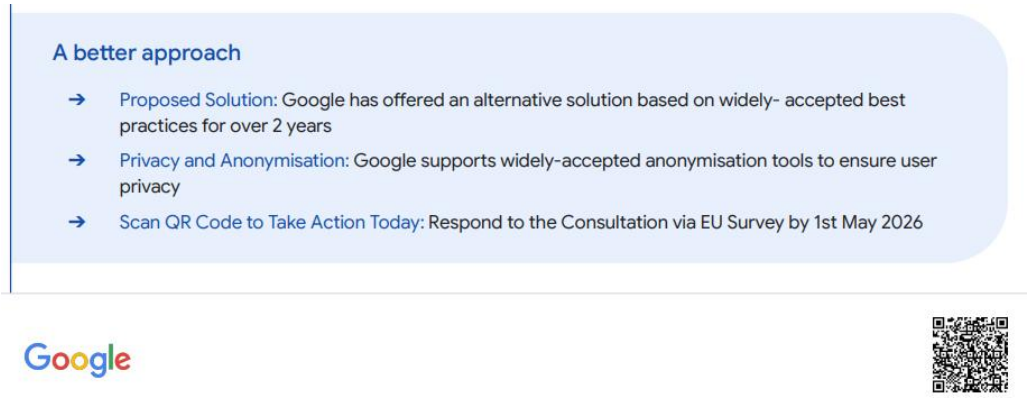
Source: Alphabet's reply to RFI 14, Annex Q1.07, Doc ID [...]

140 See for example Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.09 (Doc ID […]), and Index of annexes, Doc ID […].

141 See, for example, Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.16 (Doc ID […]), and Index of annexes, Doc ID […].

(107) The pamphlet calls for action by responding to the Public Consultation and provides a QR code leading to the Public Consultation webpage to do so (see Figure 2 below). A similar call to "*Take Action Today*" with a link to the Public Consultation web page was included in the Advertisers Concerns pamphlet.

Figure 2: Alphabet's pamphlet "Privacy Concerns"



Source: Alphabet's reply to RFI 14, Annex Q1.07, Doc ID [...]

(108) ***In the third place***, the Commission notes that at least 30 of the addressees included in Alphabet's outreach have made submissions or reached out to the Commission, most of them expressing views similar to those advocated by Alphabet.[142] In addition, a number of submissions made by third parties not specifically identified by Alphabet as addressees of its outreach repeat or paraphrase the text provided by Alphabet in its outreach document "*DMA search data sharing input"* or parts of it.[143]

(109) ***In the fourth place***, as mentioned in section 2.2 of this Decision, a number of respondents to the Public Consultation, have or have had a relationship or connection with Alphabet within the last two years or were remunerated by Alphabet for their participation in the Public Consultation.

(110) Some addressees of Alphabet's outreach shared with Alphabet their draft submission for review prior to submitting it in the Public Consultation,[144] in some cases Alphabet provided comments to the draft submission.[145] Others shared the final submission.[146] In one outreach exchange, prior to the discussion on the Public Consultation, Alphabet and the third parties discussed other types of remunerated cooperation, such as papers and events.[147] Even if those third parties were not specifically remunerated by Alphabet for their submission, it at least cannot be excluded that the potential future remuneration played a role in these third parties' decision to take part in the Public Consultation.

(111) **In conclusion**, in view of the considerations brought in this section, the Commission rejects Alphabet's claims regarding the Commission's investigation and engagement

142 See, for example, submissions in reply to the Public Consultation of [third party], Doc ID […]; [third party] referring to "*data in the wild*", Doc ID […]; [third party] (Doc ID […]) repeating the ideas and terms used in Alphabet's "*DMA search data sharing input*".

143 See, for example, submissions in reply to the Public Consultation of [third party], Doc ID […]; [third party], Doc ID […], and [third party], Doc ID […].

144 See, for example: Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.27 (Doc ID […]); Annex Q2.78 (Doc ID […]), and Annex Q2.66 (Doc ID […]).

145 See: Alphabet's reply to RFI 14 of 19 May 2026, Annexes Q2.45 (Doc ID […]) and Q2.75 (Doc ID […]).

146 See, for example Alphabet's reply to RFI 14 of 19 May 2026, Annexes Q2.52-53 (Doc ID […]); Q2.90-91(Doc ID […]).

147 See Alphabet's reply to RFI 14 of 19 May 2026, Annex Q2.55, Doc ID […].

with third parties and the Commission's compliance with the principles of good administration.

3. THE SCOPE OF ARTICLE 6(11) OF REGULATION (EU) 2022/1925

(112) Pursuant to Article 6(11) of Regulation (EU) 2022/1925, a gatekeeper must provide to any third-party undertaking providing OSEs ("**third-party OSEs**")[148], at its request, with access on FRAND terms to ranking, query, click and view data in relation to free and paid search generated by end users on its OSEs ("**Search Data**"). Any such query, click and view data that constitutes personal data must be anonymised.

(113) In relation to Article 6(11) of Regulation (EU) 2022/1925, recital 61 explains that:

(a) The value of OSEs to their respective business users and end users increases as the total number of such users increases.

(b) Undertakings providing OSEs collect and store aggregated datasets containing information about what users searched for, and how they interacted with, the results with which they were provided. Undertakings providing OSEs collect this data from searches undertaken on their own OSE and, where applicable, searches undertaken on the platforms of their downstream commercial partners. Access to the Search Data constitutes an important barrier to entry and expansion, which undermines the contestability of OSEs.

(c) Gatekeepers should therefore be required to provide access, on FRAND terms, to the Search Data to other undertakings providing OSE services, so that those third-party undertakings can optimise their services and contest the relevant CPS.

(d) Such access should also be given to third parties contracted by a provider of an OSEs who are acting as processors of this data for that OSE (hereafter referred to as "**subcontractors**").

(e) When providing access to its Search Data, a gatekeeper should ensure the protection of the personal data of end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data, without substantially degrading the quality or usefulness of the data. The relevant data is anonymised if personal data is irreversibly altered in such a way that information does not relate to an identified or identifiable natural person or where personal data is rendered anonymous in such a manner that the data subject is not or is no longer identifiable.

(114) Alphabet claims that any restrictions to fundamental rights, such as the restriction of property rights through extensive data sharing, must be based on clear and precise legal rules adopted by the competent legislator. According to Alphabet, Article 6(11) of Regulation (EU) 2022/1925 (i) is not sufficiently clear and precise to provide a valid legal basis for the allegedly expropriatory data disclosure, (ii) the Commission usurps the role of the legislator through its proposed specifications, and (iii) the specification measures exceed the boundaries of Article 6(11) of Regulation (EU) 2022/1925.[149] The Commission does not agree with this.

---

148 The term "*third-party OSEs*" includes also third parties contracted by a third-party OSE, who are acting as processors of this data for that OSE as referred to in Recital 61 of Regulation (EU) 2022/1925.

149 Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 68-79.

(115) With regard to Alphabet's first argument, the language of Article 6(11) of Regulation (EU) 2022/1925 and recital 61 of that Regulation is clear and precise. This provision clearly and precisely identifies its personal (the providers of designated OSEs) and beneficiaries (the third-party providers of OSEs). It also clearly and precisely defines the required conduct (search data sharing) by referring to industry concepts with identifiable boundaries (ranking, query, click and view data generated by end users on the OSE). It also uses established concepts to refer to the conditions of complying with the data sharing obligation (anonymised data, shared on FRAND terms). The provision is therefore clear, avoids ambiguous terms and does not feature inconsistencies.

(116) In addition, the requirement that any limitation on the exercise of fundamental rights, such as the rights of property, must be provided by the legislature itself "*does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances*" (emphasis added).[150]

(117) With regard to Alphabet's second argument, it is settled case law that, where implementing powers are conferred on the Commission, it is called upon to provide further detail in relation to the content of the legislative act in question, i.e., to specify its content, without supplementing or amending it.[151]

(118) Further, Article 8(2) of Regulation (EU) 2022/1925 explicitly empowers the Commission to specify concrete measures which companies need to adopt to comply with this provision. Article 8(8) of Regulation (EU) 2022/1925 further identifies Article 6(11) of Regulation (EU) 2022/1925 as an obligation that may require specification *via* an implementing act. This is precisely what this Decision does. Based on the specific circumstances of Google Search and Alphabet's approach to compliance, it specifies the measures Alphabet is to take in order to comply with Article 6(11) of Regulation (EU) 2022/1925.

(119) With regard to Alphabet's third argument, this Decision stays within the scope of Article 6(11) of Regulation (EU) 2022/1925 and all the measures are grounded in that Article. In particular, the Decision:

(a) specifies the definition of "*any third-party undertaking providing online search engines*" which are eligible to receive the Search Data (see section 4.2);

(b) specifies the data scope and conditions of data sharing providing more detail on "*ranking, query, click and view data in relation to free and paid search generated by end users*" on Google Search (see section 4.3);

(c) specifies anonymisation measures in line with the requirement that "*personal data shall be anonymised*" (see section 4.4);

(d) specifies "*fair, reasonable and non-discriminatory terms*" of access (see section 4.5); and

(e) specifies the process to govern access "*requests*" and non-price "*terms*" of access (see section 4.6).

---

150 Case C-817/19, Ligue des droits humains, EU:C:2022:491, paragraph 114 and C-401/19 Poland v Parliament and Council, EU:C:2022:297, paragraphs 64 and 74.

151 C-695/20, Fenix International Limited, paragraphs 44, 49; C-88/14, Commission v Parliament and Council, ECLI:EU:C:2015:499, paragraph 31.

(120) This Decision therefore falls squarely within the scope of the powers conferred by Article 8(2) of Regulation (EU) 2022/1925. In any event, the proposed specification measures do not lead to the alleged expropriation, as discussed in section 4.3.1.3.

4. MEASURES THAT THE COMMISSION IS SPECIFYING IN THIS DECISION

4.1. Overview

(121) The Commission is specifying measures that Alphabet must implement to effectively comply with Article 6(11) of Regulation (EU) 2022/1925 in relation to the following five aspects:

(a) **Eligibility of data beneficiaries:** the criteria for determining which undertakings are eligible to receive search data;

(b) **Data scope and conditions of sharing:** what data Alphabet must make available and how;

(c) **Anonymisation:** what measures Alphabet must implement to anonymise the search data, without substantially degrading the quality or usefulness of the data;

(d) **FRAND pricing of Alphabet's Search Data:** specification of the pricing framework under which the data must be made available to eligible beneficiaries; and

(e) **Process for search data acquisition and pre-acquisition testing:** the processes Alphabet must follow to allow pre-acquisition data testing, evaluate potential beneficiaries' eligibility, finalise prices and provide, suspend or terminate access to data.

4.2. Measures relating to eligibility of data beneficiaries

4.2.1. Introduction

(122) End users utilise OSE services to find information on the web, typically by entering their queries on websites or apps such as Google Search, Bing, or DuckDuckGo. An increasing trend is also the use of artificial intelligence ("**AI**") conversational agents that interact with end users through natural language, such as ChatGPT or Mistral Vibe, to find information on the web. Indeed, a number of AI chatbots already provide OSE services alongside other AI functions[152] by using their own search technology in combination with that of third-party OSE providers with whom they have entered into contracts to use their search technology (together "**AI chatbots with OSE functionalities**"). For completeness, there are also AI chatbots that do not provide OSE services but exclusively provide LLM outputs (e.g., summarising a PDF document), such as Verbum AI ("**AI chatbots without OSE functionalities**").[153]

(123) In the context of the data sharing objective of Article 6(11) of Regulation (EU) 2022/1925, several providers of traditional OSEs and AI chatbots with OSE functionalities have expressed an interest in receiving the Search Data.[154] AI chatbots

---

152 Including Google Search's AI mode. See https://search.google/ways-to-search/ai-mode/, Doc ID […], last accessed on 13 April 2026.

153 See https://verbum-ai.com/, Doc ID […], last accessed on 13 April 2026.

154 [Market participant's] reply to RFI of 18 November 2025, Doc ID […] and Doc ID […], questions 1 – 10.

without OSE functionalities have not reached out to Alphabet to request access to the Search Data.[155]

(124) Alphabet has so far concluded that companies offering AI chatbots with OSE functionalities are not eligible to receive the Search Data under Article 6(11) of Regulation (EU) 2022/1925. Alphabet concluded that they do not qualify as OSEs within the meaning of Regulation (EU) 2022/1925, but rather as virtual assistants ("**VAs**"),[156] based on, i.e., their different main "*purpose of use*" and their limited OSE functionalities in relation to navigational queries.[157]

(125) Article 6(11) of Regulation (EU) 2022/1925 provides that "*gatekeepers shall provide to any third-party undertaking providing online search engines, at its request, with access […] to ranking, query, click and view data in relation to free and paid search*." Accordingly, the Commission specifies how Alphabet must determine the eligibility of Search Data beneficiaries as follows.

4.2.2. Measures

(126) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must engage with any third-party undertaking that expresses interest in applying for eligibility to receive the Search Data (as specified in section 4.6.6.1.2.) to determine whether it is eligible to receive the Search Data following the process specified in section 4.6.6.1.2.

(127) Alphabet must share the Search Data with any third-party undertaking providing OSEs in the EU and in the EEA,[158] which meets the definition of an OSE set out in Article 2(5) of Regulation (EU) 2019/1150 and the requirements of the eligibility assessment specified in recitals (128) - (132) (an "**eligible third-party OSE**"). Alphabet must not exclude third-party undertakings, such as undertakings providing AI chatbots with OSE functionalities, to the extent that these undertakings provide an OSE meeting the definition set out in Article 2(5) of Regulation (EU) 2019/1150, even if the OSE is provided as part of a broader service.

(128) Alphabet must assess:

(a) Whether an undertaking applying for eligibility to receive Search Data (an "**undertaking applying for eligibility**")[159] is subject, directly or indirectly, to restrictive measures or other sanctions under Union law;[160] and

(b) Whether the undertaking applying for eligibility is subject, directly or indirectly, *de jure* or *de facto*, to the control of a third country that poses a

---

155 Alphabet's reply to RFI 7 of 13 March 2025, Doc ID […], question 1; Alphabet's reply to RFI 3 of 23 February 2024, Annex 1, Doc ID […], question 1; Alphabet's reply to RFI 1 of 23 November 2023, Doc ID […], question 1.

156 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1(a).

157 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 2.

158 In the EU as of today and in the EEA following the incorporation of Regulation (EU) 2022/1925 into the Agreement on the European Economic Area.

159 In other words, any undertaking that has submitted the application form specified in section 4.6.6.1.2.

160 "Restrictive measures or other sanctions" should cover economic and trade sanctions adopted on the basis of Article 29 of the Treaty on European Union or Article 215 of the Treaty on the Functioning of the European Union, as well as any other applicable law prohibiting, directly or indirectly, the conclusion of contracts for provision of services with that undertaking. For example, these include measures such as those imposed under Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 229, 31.07.2014, pages 1 – 11 or under Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP, OJ L 141, 28.5.2016, pages 79 – 124.

serious and structural non-technical cyber security risk and/or data protection risk, taking into account the following elements:

(1) The existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(2) Existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(3) The absence of effective judicial remedies, and independent and democratic control mechanisms, that can allow individuals and companies to exercise their rights to the protection of personal data and/or to correct the identified security concerns, including about existing practices referred to in point (2);

(4) Substantiated information about one or more incidents of threat actors controlled from that third country and operating out of the territory of that third country carrying out malicious cyber activities or campaigns, including phishing and theft of personal data; and

(c) Whether the undertaking applying for eligibility is an established company or credible new entrant providing an OSE as a genuine economic activity in the Union. This condition must be met only if the undertaking applying for eligibility:

(1) Either:

(a) Has provided OSE services in the Union for at least the last two consecutive years at the time of applying for eligibility; or

(b) Was founded less than two years ago but has received more than EUR 50 million in capital investments;

and

(2) Has had at least 50 000 monthly average users of its OSE services in the Union in the past year.

(129) Alphabet must conduct this assessment within the time limit specified in section 4.6.6.1.2 and in a strictly FRAND and proportionate manner. As far as practicable, Alphabet must base its assessment on publicly available information. Alphabet may only request strictly necessary additional information from undertakings applying for eligibility to the extent that such information is not publicly available and shall justify why this information is necessary. Alphabet should not require the provision of business secrets of the undertaking applying for eligibility.

(130) To this end, in accordance with section 4.6.6.1.2, Alphabet must prepare a list of FRAND and strictly necessary questions for assessing whether an undertaking applying for eligibility meets the eligibility criteria specified in this section. Alphabet may reject an undertaking as ineligible to receive Search Data if: it identifies clear and objective evidence that the undertaking is subject, directly or indirectly, to restrictive measures or other sanctions under Union law; if the undertaking is subject, *de jure* or *de facto,* to the control of a third country that poses a serious and structural

non-technical cyber security and/or data protection risk as described in recital (128)(b); or if the undertaking does not meet the above specified quantitative thresholds demonstrating that the undertaking is an established company or credible new entrant providing OSE services as a genuine economic activity in the Union.

(131) As part of its eligibility assessment, Alphabet must also inquire whether the undertaking applying for eligibility plans to process and maintain the Search Data within the EEA or whether it plans to request access via:

(a) International transfer of the Search Data to a non-EEA country on the basis of an adequacy decision of the Commission;[161] or

(b) International transfers of the Search Data on the basis of one of the relevant transfer tools foreseen in Article 46 of Regulation (EU) 2016/679 towards a non-EEA third country that is not covered by any adequacy decision.

(132) If Alphabet finds that it, as the controller and exporter of the Search Data (as specified in section 4.4.4.2.1), is unable to ensure a level of protection essentially equivalent to that guaranteed within the EEA, it must conclude that the undertaking applying for eligibility is not eligible to access the Search Data.[162]

(133) Irrespective of the eligibility criteria in recital (128), where there are credible indications that the communication of the Search Data to such undertakings may undermine the public security of the Union or its Member States, Alphabet may submit a reasoned request asking to be exempted from its obligations under Article 6(11) of Regulation (EU) 2022/1925 with respect to individual undertakings applying for eligibility. The Commission will assess this request pursuant to the exemption procedure set out at Article 10 of Regulation (EU) 2022/1925. This is without prejudice to the Commission's power to initiate the exemption procedure under Article 10 of Regulation (EU) 2022/1925 based on public security grounds on its own initiative.

(134) Neither the eligibility assessment nor the transfer impact assessment (if applicable) nor any potential reasoned request on grounds of public security may replace the condition specified in section 4.4.4.2.4.1 that all undertakings applying for eligibility must procure a Level 1 reasonable assurance report before Alphabet may grant them access to Search Data. Alphabet must not seek to substitute its eligibility assessment or transfer impact assessment (if applicable) or potential reasoned request on grounds of public security for the assessment of the independent assurance practitioner specified in section 4.4.4.2.4.1.

4.2.3. The gatekeeper's view

(135) In response to the Preliminary Findings, Alphabet argued that AI chatbots do not meet the definition of OSE laid down in Article 2(5) of Regulation (EU) 2019/1150 due to their inability to answer navigational queries and because they would not use

---

161 Transfers of personal data on the basis of an adequacy decision of the Commission adopted under Article 45 of Regulation (EU) 2016/679 do not require any additional safeguards. Adequacy decisions are made publicly available in the Official Journal and on the Commission's website here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

162 Judgment of the Court of Justice of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 and Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

the Search Data to provide OSE services.[163] Alphabet argued that AI chatbots should have been classified as VAs rather than OSEs.[164]

(136) Also in its response to the Preliminary Findings and again in its submission to the Commission regarding contractual measures dated 3 June 2026 ("**Alphabet's submission on contractual measures**"),[165] Alphabet argued that the Preliminary Findings do not include sufficient safeguards against misuse of Search Data by non-EEA state actors.[166] It argued that Alphabet should not be required to provide Search Data to third-party OSEs controlled by non-EEA state actors.[167]

(137) Alphabet further argued that foreign governments may seize Search Data through intelligence laws, citing third-party OSEs based in the United States as a particular point of concern for Alphabet.[168]

(138) In Alphabet's response to the Revised Measures, it argued that the user threshold of 50 000 monthly average users in the Union in the previous year specified in recital (128)(c)(2) was too low.[169] It argued that this would not filter out non-established providers and submitted that the threshold should be increased to a monthly average of [number] users in the last year. In support of this figure, Alphabet pointed out that the smallest OSE qualifying for Alphabet's OSE choice screen under Article 6(3) of Regulation (EU) 2022/1925 had slightly more than [number] average monthly users in the EEA.

4.2.4. The Commission's assessment

(139) As set out in section 4.2.2, the Commission specifies that any third-party undertaking providing OSEs in the EEA, as defined in Article 2(5) of Regulation (EU) 2019/1150, including AI chatbots with OSE functionalities, is eligible to receive the Search Data, provided that that undertaking also passes the eligibility assessment specified at recitals (128) – (132). In this context, the Commission has specified that Alphabet must also assess whether an undertaking applying for eligibility to receive Search Data: is subject directly or indirectly to restrictive measures or other sanctions; is subject, *de jure* or *de facto,* to the control of a third country that poses a serious and structural non-technical cyber security and/or data protection risk; or is an established company or credible new entrant operating an OSE as a genuine economic activity in the Union, assessed by means of quantitative thresholds; and intends to request Search Data under one of the relevant transfer tools foreseen in Article 46 of Regulation (EU) 2016/679.

(140) **First**, the Commission sets out below its considerations regarding the concept of OSE providers within the meaning of Article 6(11) of Regulation (EU) 2022/1925 in light of Article 2(6) thereof and in combination with Article 2(5) of Regulation (EU) 2019/1150.

(141) ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 lays down that "*the gatekeepers shall provide to any third-party undertaking providing online search engines*" access to the Search Data. It follows that the first criterion which determines whether undertakings can receive the Search Data is whether they can be

163 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraphs 553-555, 558.
164 Alphabet's response to the Preliminary Findings, Doc ID […][...] paragraphs 556-557.
165 Alphabet's submission to the Commission of 3 June 2025 regarding contractual measures, Doc ID […].
166 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 561; and Alphabet's submission on contractual measures, Doc ID […], pages 2 and 6.
167 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraphs 561 – 563.
168 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 282.
169 Alphabet's response to the Revised Measures, Doc ID […], paragraph 105.

considered as providers of OSEs in the EEA for the purposes of Regulation (EU) 2022/1925.

(142) Article 2 of Regulation (EU) 2022/1925 contains a number of definitions. However, as regards the definition of an OSE, Article 2(6) of Regulation (EU) 2022/1925 refers to Article 2(5) of Regulation (EU) 2019/1150. The latter provision states that "*online search engine*" means "*a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found*". This definition provides an exhaustive list of conditions which determine an undertaking's eligibility to benefit from Article 6(11) of Regulation (EU) 2022/1925.

(143) In addition, Article 1 of Regulation (EU) 2022/1925 establishes that the geographic scope of such Regulation is the EU. It lays down that *"[t]he purpose of this Regulation is to […] ensur[e] for all businesses contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users"* (emphasis added). However, Regulation (EU) 2022/1925 is also "*EEA-relevant*", meaning that it applies in the EEA internal market following its incorporation into the EEA Agreement, which is pending. It follows that to benefit from Regulation (EU) 2022/1925, undertakings need to be present in the EU or EEA once the Regulation is incorporated into the Agreement on the European Economic Area.

(144) Leaving aside the territorial scope of Regulation (EU) 2022/1925, Article 6(11) of Regulation (EU) 2022/1925 only requires that its beneficiaries need to be the providers of "*online search engines*". In addition, Article 6(11) of Regulation (EU) 2022/1925 uses the word "*any*" when referring to undertakings providing OSEs, without further limitation. Indeed, recital 61 of Regulation (EU) 2022/1925 explains that the objective of Article 6(11) of Regulation (EU) 2022/1925 is to remove barriers to entry and expansion in the OSE sector, so that undertakings can contest the gatekeeper OSE.

(145) Nonetheless, the Commission acknowledges that some strictly proportionate and FRAND restrictions on the pool of eligible beneficiaries are necessary for the reasons set out in recitals (157) – (183) below. These restrictions are specified in recitals (128) – (132). Other than this, any interpretation adding further criteria to the definition of OSEs is at odds with the text and objectives of Article 6(11) of Regulation (EU) 2022/1925.

(146) ***In the second place***, the fact that a given undertaking also provides additional services to OSE services does not affect its eligibility to benefit from Article 6(11) of Regulation (EU) 2022/1925. In particular, the fact that a given undertaking provides additional services or also meets another definition included in Regulation (EU) 2022/1925 does not preclude the possibility that it can equally qualify as an OSE. In order to be eligible to receive the Search Data, it is sufficient that an undertaking provides services which meet the definition of an OSE. It is immaterial that the undertaking also offers other services that may, or may not, fall within the scope of the definition of another CPS under Regulation (EU) 2022/1925. In other words, the definitions of CPSs in Article 2 of Regulation (EU) 2022/1925 are not mutually exclusive. Accordingly, nothing prevents in principle that a given service may simultaneously meet the definition of an OSE as well as, for example the definition of a VA within the meaning of Articles 2(6) and (11) of Regulation (EU)

2022/1925,[170] leaving open the conclusion on which classification best reflects the characteristics and breadth of the given service for the purpose of potential designation under Regulation (EU) 2022/1925.

(147) Notwithstanding the foregoing, Alphabet denies eligibility to receive the Search Data to undertakings which "*are not search engines*"[171] and "*appear[] to be better classified as [] virtual assistant[s]*",[172] because in Alphabet's view their "*primary purpose*" is not the one of an OSE.[173] Alphabet's reference to this criterion is misplaced and incorrect. In particular:

(a) Alphabet's argument that "*where a service "displays features of" two services […], the correct approach is to classify the service based on the "broader definition" […] and not as a service with the "narrower definition*"[174] is unsupported. Contrary to Alphabet's claim that the Commission needs to determine whether a service meets one definition over another (i.e., exclusive alternative),[175] the *ByteDance* designation decision, which was upheld by the General Court,[176] demonstrates that it is possible that two legal definitions are overlapping and a given service can meet both of them at the same time (i.e., inclusive alternative).[177] In particular, this decision found that TikTok met both the definition of online social network and the definition of video sharing platform, and then concluded that for the purposes of designation under Regulation (EU) 2022/1925, TikTok could be regarded as the online social network CPS.[178] The conclusion that TikTok could be regarded as the online social network for designation purposes did not preclude that TikTok also met the definition of video sharing platform and could therefore become the beneficiary of a hypothetical gatekeeper's obligations vis-à-vis video sharing platforms.

(b) As the point (a) above demonstrates, contrary to Alphabet's allegation, the Commission does not "*attempt to distance themselves from [their] own*

---

170 That is without prejudice to the consequences to be drawn from that circumstance for the purposes of the designation of an undertaking as a gatekeeper providing OSE services, VA services or even both.

171 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraphs 552-560.

172 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1.

173 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1. As Alphabet refers to the criteria "*centre of gravity*" and "*primary purpose*" as synonyms. These Preliminary Findings refer to these concepts joint as "*primary purpose*" for brevity.

174 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1. See also Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 556.

175 Ibidem.

176 ByteDance Designation Decision, Commission decision C(2023) 6102 ("**ByteDance Designation Decision**").

177 See ByteDance Designation Decision, paragraph 48: "*Regulation (EU) 2022/1925 does not preclude the possibility that a service falling within the broader definition of online social networking services laid down in Article 2, point (7), of Regulation (EU) 2022/1925 may also meet the narrower definition of video-sharing platform services laid down in Article 2, point (8), of that Regulation*".

178 See ByteDance Designation Decision, paragraph 42: "*The Commission does not contest that, in line with ByteDance's view, TikTok meets the definition of a video-sharing platform service within the meaning of Article 2, point (8), of Regulation (EU) 2022/1925 because an essential functionality of that service is devoted to user-generated videos. However, the Commission considers that the features and functionalities of TikTok go beyond those of a video-sharing platform service. As explained in recitals (43) to (65) below, the Commission considers that TikTok not only fulfils the definition of an online social networking service, but that that classification also best reflects the characteristics and breadth of TikTok's features and functionalities. Consequently, the Commission considers that TikTok constitutes an online social networking CPS*". The General Court of the EU upheld the Commission's decision C(2023) 6102 in its entirety in the judgment of 17 July 2024 in Case T-1077/23 – Bytedance v Commission, EU:T:2024:478.

ByteDance decision."[179] The key distinction lies in differentiating between two separate issues: (i) whether a service meets a simple legal definition, and (ii) whether it qualifies as a specific CPS for the purpose of designation under Regulation (EU) 2022/1925. The latter has broader implications as it subjects CPSs to numerous legal obligations under Regulation (EU) 2022/1925. It requires the application of numerous criteria listed under Articles 3(1), (2) and (8) of Regulation (EU) 2022/1925 and may also require assessing the "*primary purpose*" of a service as done in the particular case of TikTok.[180] This reasoning is reflected in the *ByteDance* decision, in which the Commission (i) first analysed legal definitions met by TikTok concluding that it meets two of them, and (ii) only later discussed its designation as a CPS, concluding that, for that purpose, the definition as an online social networking service best reflected the characteristics and breadth of TikTok's features and functionalities. The assessment made for the purpose of this Decision is a different one limited to concluding that AI chatbots with OSE functionalities meet the definition of OSE for the purpose of qualifying as an eligible beneficiary of Article 6(11) of Regulation (EU) 2022/1925. The Commission does not conduct a different assessment of their CPS classification for designation purposes, leaving this question open.

(148) Alphabet also motivates its refusal to share the Search Data with AI chatbots with OSE functionalities because of the marketing of such chatbots as AI assistants rather than as AI OSEs.[181] As a matter of principle, and as explained in recitals (141)-(142) above, this criterion finds no basis in the OSE definition set out in Article 2(5) of Regulation (EU) 2019/1150. If Alphabet were to adopt it to assess the eligibility of undertakings to benefit from Article 6(11) of Regulation (EU) 2022/1925, it would effectively narrow the personal scope of that provision to a small group of beneficiaries, contrary to the letter and the spirit of that provision. Furthermore, the subjective character of these criteria would confer on Alphabet a discretionary power to arbitrarily determine which undertakings can benefit from Article 6(11) of Regulation (EU) 2022/1925.[182] In any event, some AI chatbots also market their search functionality.[183]

(149) **Second**, the Commission takes the view that AI chatbots with OSE functionalities are to be regarded as OSEs for the purposes of Article 6(11) of Regulation (EU) 2022/1925 in light of Article 2(6) thereof and in combination with Article 2(5) of Regulation (EU) 2019/1150 for the cumulative reasons set out below. For

---

179 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 557.

180 The principle of "*primary purpose*" follows from the application of Section D, paragraph 2(b) of the Annex to Regulation (EU) 2022/1925, which states that "*undertaking providing core platform service(s) shall consider as distinct core platform services those core platform services, which are used for different purposes by either their end users or their business users, or both*". The ByteDance Designation Decision further adds "*different services may constitute a single CPS, if they are used for the same purpose from both an end user and a business user perspective, unless they belong to different categories of the CPSs listed in Article 2, point (2), of Regulation (EU) 2022/1925.*" (paragraph 12).

181 Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1.

182 This concern is also raised in public consultation responses. See the submission by [third party], Doc ID […]: *"At the same time, the proposed framework appears to leave a significant role to the gatekeeper in assessing eligibility. From an economic standpoint, this raises a clear risk of foreclosure through procedural or informational asymmetries, as access conditions could be used strategically to limit entry"* (emphasis added).

183 See, e.g., https://openai.com/index/introducing-chatgpt-search/, Doc ID […], last accessed on 13 April 2026; https://helpagemistral.ai/en/articles/424369-browse-the-web-with-le-chat, Doc ID […], last accessed on 13 April 2026.

completeness, AI chatbots without OSE functionalities, which do not provide OSE services but exclusively provide LLM outputs (e.g., summarising a PDF document) are not considered eligible beneficiaries for the purpose of this Decision.[184]

(150) ***In the first place***, AI chatbots have OSE functionalities when they are "*digital service[s]*" within the meaning of Article 2(5) of Regulation (EU) 2019/1150. That is, they use digital technology, such as computer systems, and the internet as part of their service.

(151) ***In the second place***, AI chatbots have OSE functionalities when they "*allow users to input queries […] on any subject, in the form e.g., of a keyword, voice request, phrase or other input*" within the meaning of Article 2(5) of Regulation (EU) 2019/1150. The interaction with such AI chatbot begins with a user entering a query, exactly as in the case of traditional OSEs. Users can enter queries on any subject, e.g., travel, history, business, celebrities, etc. They can also input queries in different forms, e.g., they can input text or voice queries. This conclusion is not put into question by Alphabet's claim that AI chatbots with OSE functionalities are allegedly unable to respond to navigational queries.[185] In particular:

(a) The reference to queries "*on any subject*" in Article 2(5) of Regulation (EU) 2019/1150 refers to the semantic focus of the query, meaning the topic of the query and concepts that form part of search, rather than the classification based on user intent, which includes navigational queries.[186] The idea that an OSE should be able to answer to questions on any topic is also confirmed by the rest of Article 2(5) of Regulation (EU) 2019/1150, which refers to the ability of OSEs to perform searches of "*all websites*", implying that they need to have general search ability rather than be able to only answer specialised queries not performing searches of "*all websites*" (e.g., queries regarding hotels, flights, real estate, scientific knowledge).[187] AI chatbots that have this general search ability and can answer queries on any subject, no matter whether it relates to finance, medicine, commerce, history, etc., can be considered AI chatbots with OSE functionalities.

---

184 Public consultation responses provided mixed views on whether AI chatbots should be eligible to receive the Search Data. However, the submissions focused on policy considerations rather than legal analysis. In favour of giving AI chatbots with OSE functionalities the right to access the Search Data: [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […]. Against: [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […], [third party], Doc ID […].

185 According to Alphabet, *"[n]navigational queries are queries where the user is looking for a specific website destination and enters the name of the website into a search engine to obtain the link to that website*". See Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1. See also Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraphs 553-555.

186 See https://sites.uef.fi/tiedonhaku-kirjasto/from-a-topic-into-a-search-query/?lang=en&utm_source, Doc ID […], last accessed on 21 May 2026. According to Alphabet, *"[n]navigational queries are queries where the user is looking for a specific website destination and enters the name of the website into a search engine to obtain the link to that website*". See Alphabet's reply to RFI 9 of 22 July 2024, Doc ID […], question 1. See also Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 554.

187 This condition addresses the concern expressed in public consultation responses that OSEs active in a single sector (e.g., medical) should not be eligible to receive the Search Data. See the submission by [third party], Doc ID […]; [third party], Doc ID […]; and [third party], Doc ID […]. Against this, see submissions by [third party], Doc ID […]; and [third party], Doc ID […].

(b) AI chatbots have OSE functionalities when they are also able to cater for navigational queries, contrary to Alphabet's allegation.[188] They either directly include links in reply to user queries or users can ask in their queries to be provided with links, or users can personalise their request to always receive links in settings. For example, in [market participant's website], users can enter an instruction *"when you see only the name of a website as an input, provide me the main web link to visit the website"* in *"custom instructions"*.

(152) ***In the third place***, AI chatbots have OSE functionalities when they "*perform searches of, in principle, all websites, or all websites in a particular language*" in line with Article 2(5) of Regulation (EU) 2019/1150. AI chatbots with OSE functionalities can perform searches of "*in principle, all websites*", exactly as traditional OSEs. They perform their services based on a combination of their own search technology and on syndication or similar contracts, which can cover in principle the whole web and are not subject restricted.[189] For example, they may combine own search results with the results from their syndication partners, decide on the ranking of search results and design of SERP based on their own search technology.[190] The search of "*in principle, all websites*" is therefore effectively carried out through a combination of own and third-party search infrastructure.

(153) In particular, the AI chatbots' OSE technology may be generally characterised as follows:

(a) AI chatbots with OSE functionalities have a dual character, with the search and LLM components being their two complementary technological foundations.[191]

(b) The LLM component is a type of artificial neural network that generates human-like language responses. Its main function is to generate text or other creative output based on user's query. The LLMs behind AI services have been trained on historic datasets, which have a knowledge cut-off.[192]

(c) The search component is a technology that allows AI chatbots with OSE functionalities to check the current state of the internet (so-called "**grounding**") to retrieve new information and avoid factually incorrect or misleading statements (so-called "**hallucinations**").[193] The search component (a commonly used architecture of such search is retrieval-augmented generation ("**RAG**"))[194] is responsible for retrieving relevant information from the internet, matching user's query with relevant websites and ranking them.

(d) The search and LLM technologies are independent components, with different functions. For example, [market participant] used to offer to users the

188 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraph 554.

189 [Market participant's] submission dated 2 October 2025, Doc ID […]; [Market participant's] testimony in Case No. 20-cv-3010 (APM) US v. Google LLC, ("**US vs. Google***")*, Doc ID […], page 394-407.

190 Australian Competition & Consumer Commission, Digital platform services inquiry - September 2021 interim report, page 130, available at https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-september-2021-interim-report, Doc ID […], last accessed on 13 April 2026.

191 [Market participant's] testimony in US vs. Google, Doc ID […]page 388; agreed minutes of meeting with [market participant] of 13 June 2024, Doc ID […], page 3.

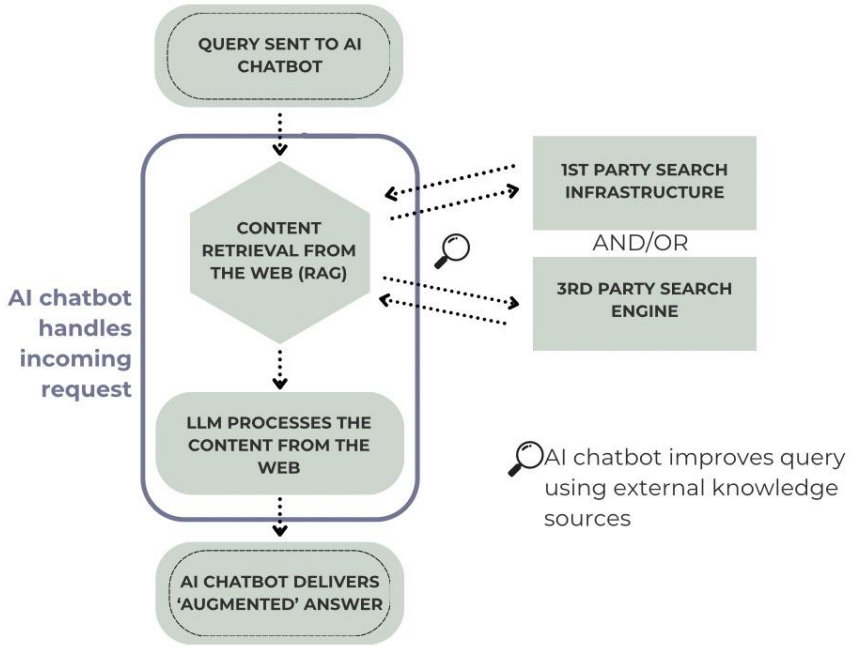
192 [Market participant's] testimony in US vs. Google, Doc ID […], page 382.

193 [Market participant's] testimony in US vs. Google, Doc ID […] page 383 and 413; market participant's presentation dated 12 February 2026, Doc ID […], page 5.

194 Grounding is a means to connect an LLM to external information. RAG is a commonly used grounding architecture, which retrieves external documents and augments the initial prompt with those before generating a response. Market participant's reply to RFI PO 1 of 17 February 2026, Doc ID […], question 1.

prototype of its search component, [name], on a stand-alone basis before it integrated it into the core [name] product.[195] The search component and the LLM components are, however, used in sequence[196] to produce a single output as illustrated in Figure 3 below.

Figure 3: Search grounding of AI chatbots



Source: Own illustration

(e) Focusing on the search component of AI chatbots with OSE functionalities, it does not differ from that of traditional OSEs:

(1) Firstly, the search technologies of AI chatbots with OSE functionalities correspond to the structure of a typical OSE. For example, [market participant's] search technology involves several main interconnected components that work together to crawl the web, index websites, process user queries, retrieve matching results, rank them and serve them to the user.[197]

(2) Secondly, AI chatbots with OSE functionalities may rely on a combination of own search technologies and third-party technologies, similarly to traditional OSEs. For example, [market participant] is currently developing its own OSE,[198] to be integrated in [market participant's service], with a view to serving approximately 80 percent of its traffic from its own search index.[199] In such a case the own search component is complemented with a syndicated search results – which are regularly used also by traditional OSEs that do not rely only on their search technology. When syndicated search results are required the AI chatbots with OSE functionalities sends some queries to a third-party

195 [Market participant's] testimony in US vs. Google, Doc ID […], page 420.
196 [Market participant's] testimony in US vs. Google, Doc ID […] page 401.
197 [Market participant's] testimony in US vs. Google, Doc ID […], page 360.
198 Agreed minutes of meeting with [market participant] of 21 May 2025, Doc ID […], paragraph 8.
199 [Market participant's] testimony in US vs. Google, Doc ID […], page 394.

OSE and it receives a list of search results, processes them through own OSE technologies and then feeds them into the LLM.[200]

(154) ***In the fourth place***, AI chatbots have OSE functionalities when they "*return results in any format in which information related to the requested content can be found*". In this context AI chatbots with OSE functionalities, like OSEs, return "*search results*" within the meaning of Article 2(23) of Regulation (EU) 2022/1925, which refers to "*any information in any format, including textual, graphic, vocal or other outputs, returned in response to, and related to, a search query, irrespective of whether the information returned is a paid or an unpaid result, a direct answer or any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*" (emphasis added).

(155) **Third**, the Commission observes that its market investigation did not confirm Alphabet's allegation that AI chatbots with OSE functionalities would mostly use the Search Data for non-OSE related uses.[201] Potential beneficiaries confirmed that they are planning to use the Search Data for optimising their OSE services, including to better understand user queries, to identify more responsive search results to user queries based on user interaction data, and to update their search index to include most popular websites, all of which are also typical use cases for traditional OSEs.[202] In any event, the Decision restricts the use of Search Data to OSE-related uses, with contractual obligations requiring beneficiaries to comply. Breach of this provision may result in termination of Search Data sharing (see further section 4.4.4.2).[203]

(156) The Commission concludes that undertakings' eligibility to receive the Search Data is exclusively determined by meeting the definition of an OSE, as set out in Article 2(5) of Regulation (EU) 2019/1150. The Commission finds that AI chatbots with OSE functionalities, as defined above (recitals (150)-(154)), meet this definition and qualify as beneficiaries of Article 6(11) of Regulation (EU) 2022/1925. This is without prejudice to AI chatbots with OSE functionalities potentially meeting other definitions included in Regulation (EU) 2019/1150, which is immaterial for the present purposes.

(157) **Fourth**, the Commission sets out below its reasons for specifying that Alphabet must conduct a strictly FRAND and proportionate eligibility assessment and also provides further guidance on how Alphabet must interpret this requirement.

(158) ***In the first place***, the eligibility assessment specified above is intended to filter out:

(a) Undertakings that are subject, directly or indirectly, to restrictive measures or other sanctions under Union law; or

(b) Undertakings that are subject, directly or indirectly, *de jure* or *de facto*, to the control of a third country that poses a serious and structural non-technical cyber security risk and/or data protection risk; or

(c) Undertakings applying for eligibility that cannot provide and substantiate basic indications that they are established companies or credible new entrants with

200 [Market participant's] testimony in US vs. Google, Doc ID […], page 400-407.

201 Alphabet's response to the Preliminary Findings, Doc ID […][...], paragraphs 558-559.

202 Market participant's presentation of 12 February 2026, Doc ID […], page 10; market participant's reply to RFI PO 1 of 17 February 2026, Doc ID […], question 1; [Market participant's] reply to RFI PO 1 of 18 November 2025, Tranche 1, Doc ID […], question 2.

203 This also addresses the comments received in public consultation responses on the need to ensure that the Search Data are used for OSE activities by undertakings whose business models extend beyond OSEs. See the submissions from [third party], Doc ID […], [third party], Doc […], [third party], Doc ID […].

either existing experience in handling sensitive OSE data or financial capacity to develop independent OSE services and handle the resulting sensitive data.

(159) The Commission therefore expects Alphabet to conduct this assessment based on FRAND and strictly objective criteria as a "*first line of defence*" to exclude undertakings that are clearly unsuitable to receive Search Data.

(160) In this regard, the Commission has specified at section 4.4.4.2.2.1 a contractual measure entitled *"permitted purposes of use"*. In the Commission's assessment, undertakings subject, directly or indirectly, to restrictive measures or other sanctions under Union law present a high risk of misusing Search Data beyond the permitted purposes of use.

(161) An undertaking applying for eligibility should be understood to be subject, directly or indirectly, to restrictive measures or other sanctions under Union law if:

(a) The undertaking or any natural or legal person controlling that undertaking is designated as a sanctioned entity under Union law;[204] or

(b) There are other restrictive measures or sanctions under Union law which otherwise prohibit the provision of Search Data or related goods and services to the undertaking applying for eligibility or any natural or legal person controlling that undertaking.[205]

(162) Besides, the Commission notes that Alphabet argued that it should be given further powers to exclude undertakings applying for eligibility based on public security grounds at international level.[206] Moreover, some responses to the Public Consultation called on the Commission to include further eligibility criteria to exclude third-party OSEs on similar public security grounds.[207] The Commission

---

204 "Restrictive measures or other sanctions" should cover economic and trade sanctions adopted on the basis of Article 29 of the Treaty on European Union or Article 215 of the Treaty on the Functioning of the European Union, as well as any other applicable law prohibiting, directly or indirectly, the conclusion of contracts for the provision of services with that undertaking. For example, these include measures such as those imposed under Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 229, 31.07.2014, pages 1 – 11 or under Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP, OJ L 141, 28.5.2016, pages 79 – 124.

205 In other words, an undertaking applying for eligibility might not be designated on any sanctions list under the restrictive measures or other sanctions laws of the Union. However, restrictive measures might nonetheless prohibit provision of Search Data or related goods and services (for example, advertising services, audit services or platforms for training AI models) to that undertaking as it is established in a jurisdiction subject to restrictive measures under Union law. In this scenario, Alphabet must deem the undertaking applying for eligibility as ineligible.

206 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 561 – 564.

207 See responses to the Public Consultation of: [third party] – *"IV. Geopolitical Concerns: The proposed measures also raise broader geopolitical and strategic concerns, particularly in light of the scope of entities that may be eligible to receive search data … The sharing requirements laid out in the preliminary findings do not account for ownership structure, jurisdictional affiliation, or the broader data ecosystem in which those entities operate"*, Doc ID […]; [third party] – *"The criterion of operating a search engine in the EEA on its own [is] unlikely to deter sophisticated actors operating through formally compliant intermediaries."*, Doc ID […]; [third party] – "*We are equally concerned about the potential negative consequences for national security",* Doc ID […]; [third party] – *"Given the geopolitical sensitivity of behavioural search data, this assessment should be mandatory ("shall"), not optional"*, Doc ID […], and [third party] – *"Eligibility should exclude entities that primarily use data for … political targeting, law enforcement support, or intelligence-related purposes"*, Doc ID […].

considers it appropriate to address those concerns[208] by specifying eligibility criteria targeting undertakings that are subject, directly or indirectly, *de jure* or *de facto*, to the control of a third country that poses a serious and structural non-technical cyber security risk and/or data protection risk. Such undertakings may be subject to legal obligations or established practices capable of undermining the effectiveness of the technical and contractual measures specified in this Decision (section 4.4). In particular, the objective criteria specified in recital (128)(b) identify situations in which legal framework, institutional safeguards or established practices of a third country create a heightened risk that the Search Data could be exposed to unauthorised access, disclosure or other processing incompatible with the objectives of Article 6(11) of Regulation (EU) 2022/1925. It is therefore appropriate to require Alphabet to exclude from eligibility undertakings subject to such control, on the basis of the objective criteria specified in recital (128)(b).

(163) Moreover, undertakings that cannot provide and substantiate basic indications that they are established companies or credible new entrants with either existing experience in handling sensitive OSE data or financial capacity to develop OSE services and handle such sensitive data should be excluded from receiving Search Data. In that regard, under the first assurance objective specified at section 4.4.4.2.4.1.3, the independent assurance practitioner must verify that a third-party OSE has adequate resourcing for implementing or preserving the anonymisation of the Search Data. It is appropriate to enable Alphabet (while not supplanting the role auditor in the independent verification mechanism) to filter out undertakings that are highly unlikely to satisfy that assurance objective, on the basis of the above specified objective criteria indicating that they are not established providers of OSE services or credible entrants in the provision of OSE services.

(164) Accordingly, to ensure the effectiveness of these measures, Alphabet must put in place a process for excluding as ineligible to receive Search Data undertakings that are subject to restrictive measures or other sanctions under Union law or to control of a third country that poses a serious and structural non-technical cyber security and/or data protection risk, or fail to meet the quantitative thresholds specified at recital (128)(c).

(165) ***In the second place,*** it is appropriate to require Alphabet to assess whether the undertaking in question is an established company or credible new entrant operating an OSE service as a genuine economic activity in the Union. The Commission has specified that this condition will be met only if the undertaking applying for eligibility has: either operated an OSE in the Union for at least the last two consecutive years or is less than two years old but has received more than EUR 50 million in capital investments; and in either case has had at least 50 000 monthly average users of its OSE services in the Union in the past year.

(166) The Commission received a number of different views in response to the public consultation on whether Search Data should be made available to new entrants providing OSE services, or whether it should be limited to established players. Some respondents submitted that Search Data should be available to new and potential entrants that are planning to offer OSE services in the Union.[209] These responses

---

208 For similar concerns, see for example, article 100 of the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2), COM (2026) 11 final.

209 Responses to the public consultation of: [third party] – *"In our view it is necessary to clarify that "undertakings providing online search engines" ... do not only include undertakings that are already*

emphasised that new entrants could be a source of competitive pressure contributing to contestability in OSE services.[210] One such response suggested that the Commission should specify measures to give Alphabet discretion to allow *"credible entrants"* into OSE services to access the Search Data.[211]

(167) On the other hand, a number of consultation responses stressed that eligibility should only be open to undertakings with a verified history of operation and substantial user base in the Union.[212]

(168) The Commission considers that these competing perspectives have merit and the quantitative thresholds the Commission has specified at recital (128)(c) strike an appropriate balance between them. Established (even if relatively small) providers of OSE services, should in principle be eligible to access the Search Data, thereby contributing to contestability in online search. The Commission has therefore specified a set of eligibility thresholds designed to ensure that only genuine providers of OSE services in the Union access Search Data, while ensuring that these barriers are placed at an appropriately low level to foster contestability and fairness.

(169) At the same time, in fast-moving and highly innovative sectors such as the provision of OSE services, the Commission recognises that two years of activity may be too high a barrier for some credible new entrants, who might be able to grow quickly with the benefit of Search Data, allowing them to contest the position of Google Search. The Commission considers that providers of OSE services with a demonstrated capacity to seek substantial investment should also be eligible to receive Search Data. Such investment demonstrates *prima facie* that the undertaking in question is a credible provider offering a promising product. Therefore, the Commission has specified that undertakings active for less than two years may

---

active on the market but also include potential competitors, especially micro enterprises, Start-ups, and SMEs, that are demonstrably developing online search engines and planning market entry in Europe", Doc ID […]; and [third party] – *"We recommend that credible entrants into search should also receive access to data"*, Doc ID […].

210 Responses to the public consultation of: [third party] – *"In order to enable competition on the market for online search engines, existing entry barriers must be significantly lowered. Barriers especially arise from network effects…. Granting access only to those players that are already active on the market does not sufficiently foster competition and contradicts the "effet utile" principle"* Doc ID […]; [third party] – *"Credible entry can be its own source of competitive pressure and therefore contribute to the objective of contestability. Extending the scope is better in line with Rec. 28 DMA: "it should also reassure actual or potential market participants about the contestability and fairness of the services concerned.""* Doc ID […]; and [national public authority] – *"From a competition perspective, search markets are characterised by strong indirect network effects and cumulative data advantages, whereby scale in user interactions continuously reinforces the quality of the service and entrenches incumbency…. In this respect, we encourage the European Commission to specify more precisely how it would make sure that Google effectively addresses all third-party undertakings…."* Doc ID […].

211 Response to the public consultation of [third party] – *"Alphabet should be permitted to determine, within reason, whether the claim of entry into the search market is credible for potential entrants, but potential entrants should not be pre-emptively excluded from access through the specification decision itself."* Doc ID […].

212 See responses to the public consultation of: [third party] – *"Eligibility controls should be significantly strengthened. At minimum, they should include: verified operational history as a genuine search product with substantial EU user base"* Doc ID […]; [third party] – *"Eligibility should be restricted to substantial, well-established bona-fide public search engines only. In particular, private or otherwise restricted search engines should be excluded even if they fulfil the Art 2(5) definition. Furthermore, eligibility criteria should be crafted to resist attempts by obscure operators to use Art 2(5) definition as pretext for gaining access to search data. Only bona-fide public search engines should gain access"* Doc ID […]; and [third party] – *"Restrict eligibility to general-purpose search engine providers with a demonstrated, existing search index and minimum operational history in the EU"*, Doc ID […].

access Search Data if they can demonstrate that they have received more than EUR 50 million in capital investments.

(170) These thresholds also avoid granting Alphabet an undue degree of discretion over third-party OSEs' eligibility to receive Search Data. As a number of responses to the public consultation highlighted, granting too much discretion to Alphabet over eligibility and Search Data access increases the risk of foreclosure, which could undermine contestability.[213]

(171) However, the Commission has decided not to accept the request in Alphabet's response to the Revised Measures to increase the monthly user threshold to [number] average monthly users in the past year. In this regard, Alphabet's reliance on the user numbers of the smallest third-party OSE qualifying for its OSE choice screen under Article 6(3) of Regulation (EU) 2022/1925 is misplaced. Article 6(3) of Regulation (EU) 2022/1925 obliges gatekeepers to *"[prompt] … end users … to choose, from a list of the main available service providers, the online search engine … to which the virtual assistant and the web browser of the gatekeeper directs or steers end users by default*(Emphasis added). That Article therefore explicitly identifies its beneficiaries as only the *"main providers"* of OSE services.

(172) By contrast, there is no such reference in Article 6(11) of Regulation (EU) 2022/1925. The text of Article 6(11) of Regulation (EU) 2022/1925 therefore does not oblige the Commission to restrict the pool of beneficiaries of that Article to only the *"main"* third-party OSEs. Moreover, recital 61 of Regulation (EU) 2022/1925 makes clear that the requirement to share Search Data with third-party OSEs is necessary to enable them to contest the position of Google Search by lowering barriers to entry and expansion. In light of this and the competing concerns identified in the recitals above, the Commission is justified in applying a monthly end user threshold of 50 000 end users in the past year as this threshold is appropriate for its objective as described at recitals (165) – (170).

(173) The Commission acknowledges that some genuine and credible new entrants in OSE services will be unable to meet these quantitative thresholds. However, a significant pool of third parties providing OSE services will nonetheless have access to the Search Data, enabling many players to contest the position of the Google Search. In addition, it is possible that some third party OSEs in receipt of Search Data may offer search syndication to new entrants and smaller third-party OSEs. Potential improvements in the quality, price and supply of syndication arrangements on offer may enable these new entrants and smaller third-parties OSEs to increase their user numbers in the Union, thereby giving them the chance in future to meet these quantitative thresholds and later access the Search Data.

(174) ***In the third place,*** the Commission has taken note of Alphabet's submission in its response to the Preliminary Findings that foreign governments may access Search

---

213 Responses to the public consultation of: [national public authority] *"…the proposed framework appears to leave a significant role to the gatekeeper in assessing eligibility. From an economic standpoint, this raises a clear risk of foreclosure through procedural or informational asymmetries, as access conditions could be used strategically to limit entry. In our view, eligibility criteria should therefore be interpreted broadly and applied under strict supervisory conditions, ensuring that the gatekeeper cannot exercise discretionary control over access. This is a necessary condition for the measure to effectively contribute to market contestability"*, Doc ID […]; [third party] – *"This framework raises concerns regarding governance and oversight. It assigns Alphabet a central operational role that includes decision-making authority over access…. Although procedural safeguards limit this discretion, Alphabet retains a degree of unilateral decision-making that may create issues in the event of disagreements with third-party OSEs"*, Doc ID […].

Data under their intelligence laws.[214] In this regard, the Commission considers that Alphabet must incorporate the necessary due diligence questions into its eligibility assessment[215] with a view to ensuring that Alphabet is in a position to ensure that any international Search Data transfers to an undertaking applying for eligibility occur in compliance with Chapter V of Regulation (EU) 2016/679 in accordance with the measure provided in recital (795)(b) where the sharing of the Search Dataset remains a processing of personal data subject to the protection of Regulation (EU) 2016/679 as explained in section 4.4.4.2.1. This ensures that the Search Data will only be transferred to jurisdictions providing an adequate level of protection or on the basis of appropriate safeguards ensuring a level of protection essentially equivalent to that guaranteed within the EEA:[216]

(a) The Commission recalls that in line with Articles 44 to 46 of Regulation (EU) 2016/679 Alphabet shall only provide access to the Search Dataset to a third-party OSE recipient via international transfer(s) to a non-EEA country on the basis of an adequacy decision of the Commission[217] or, in the absence of such a decision, on the basis of one of the relevant transfer tools foreseen in Article 46 of that Regulation providing appropriate safeguards including enforceable rights and effective legal remedies for individuals.[218] If the third-party OSE requests access to the Search Dataset via international transfers on the basis of an adequacy decision of the Commission, Alphabet should not impose any additional safeguards or measures in that regard. In particular, third-party OSEs that have adhered to the EU-US Data Privacy Framework and request transfer of the Search Data under that Framework should not be subject to additional scrutiny by Alphabet as the Commission Implementing Decision EU 2023/1795 of 10 July 2023 provides that that Framework ensures an adequate level of protection of the data transferred to the US.[219]

(b) If the third-party OSE requests access to the Search Dataset via international transfers on the basis of one of the relevant transfer tools foreseen in Article 46 of that Regulation towards a non-EEA third country that is not covered by any adequacy decision, the Court of Justice has stated that the data controller acting

---

214 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 282(c) and footnote 114. See also response to the public consultation from [third party] – *"Given the intelligence value ... the Commission should assess whether the eligibility framework should incorporate additional due diligence requirements addressing the risk that formally compliant applicants may be instruments of foreign state intelligence collection"*, Doc ID […].

215 By incorporating questions into the application form specified at section 4.6.6.1.2 necessary to verify whether a transfer impact assessment is required. If no transfer impact assessment is required, Alphabet must not ask the transfer impact assessment questions to any undertaking applying for eligibility. If such an assessment is required, Alphabet may then pose the necessary transfer impact assessment questions to the undertaking applying for eligibility in question.

216 Judgment of the Court of Justice of 6 October 2015, Maximilian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 and Judgment of the Court of justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

217 Transfers of personal data on the basis of an adequacy decision of the Commission adopted under Article 45 of Regulation (EU) 2016/679 do not require any additional safeguards. Adequacy decisions are made publicly available in the Official Journal and on the Commission's website here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

218 For the avoidance of doubt, the Search Dataset cannot be transferred under any derogation provided under Article 49 of Regulation (EU) 2016/679.

219 Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ L 231, 20.9.2023, pages 118 - 229.

as exporter (here Alphabet as explained in section 4.4.4.2.1) is responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data (i.e. undertaking applying for eligibility), whether the law or practice of the non-EEA country impinges, for example due to legislation imposing access to data by public authorities, on the effectiveness of the appropriate safeguards contained in the transfer tool relied on in accordance with Article 46 of Regulation (EU) 2016/679.[220] In practice, this translates into a requirement to carry out a transfer impact assessment documenting the specific circumstances of the transfer, the laws and practices in the third country of destination as regards access by the public authorities to the personal data transferred as well as the relevant aspects of the legal system of that third country.[221] In that context, Alphabet must include all necessary due diligence questions into its eligibility assessment to determine whether it is required to carry out that transfer impact assessment. In the specific circumstances where a transfer impact assessment is required, Alphabet must issue the necessary questions for a transfer impact assessment to the undertaking applying for eligibility in question. Where Alphabet, as the exporter of the Search Dataset, is not able to take adequate additional measures to guarantee that the transfer tool relied on provides a level of protection essentially equivalent to that guaranteed within the EEA, it must consider that undertaking ineligible since Alphabet is required to not transfer the Search Dataset to the third country concerned.[222]

(175) It follows from the above that Regulation (EU) 2016/679 provides a comprehensive framework ensuring that no Search Data transfers can occur to a third country under conditions that would not guarantee a level of protection of the Search Data essentially equivalent to that guaranteed in the Union.

(176) ***In the fourth place***, the Commission considers it necessary to specify that this assessment must:

(a) Be FRAND, strictly proportionate and confined only to the matters specified at recitals (128) – (132);

(b) Be based as far as practicable on publicly available information, with Alphabet only entitled to request strictly necessary additional information from undertakings applying for eligibility to the extent that such information is not publicly available, justifying why this information is necessary for the eligibility assessment; and

(c) Not require the sharing of business secrets of the undertaking applying for eligibility.

(177) In this regard, the Commission notes that in response to the public consultation, several respondents expressed concern that Alphabet could use procedural rules to unfairly, unreasonably or discriminatorily prevent third-party OSEs from effectively

---

220 Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraphs 104-105, 133-135.

221 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021 and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures of 10 November 2020.

222 Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 135.

accessing Search Data and called for greater restrictions on Alphabet's procedural discretion to avoid such eventualities.[223]

(178) If Alphabet were permitted to add eligibility criteria or otherwise conduct an expansive eligibility due diligence process beyond what is specified at recitals (128) - (132), this could constitute a disproportionate restriction on third-party OSEs' ability to exercise their right to access Search Data on FRAND terms under Article 6(11) of Regulation (EU) 2022/1925, thereby undermining contestability in online search.

(179) Finally, the Commission notes that, if Alphabet were entitled to access business secrets of undertakings applying for eligibility, it could give Alphabet an unfair competitive advantage over those undertakings, thereby undermining contestability and fairness in the provision of OSE services. The limitation on Alphabet's possibility to require the provision of business secrets from third parties is therefore justified.

(180) **Fifth**, without prejudice to the ordinary eligibility assessment specified at recitals (128) - (132), Alphabet may submit a reasoned request asking to be exempted on grounds of public security from its obligation under Article 6(11) of Regulation (EU) 2022/1925 with respect to a specific undertaking applying for eligibility.

(181) Article 10 of Regulation (EU) 2022/1925 provides a legal basis for exempting a gatekeeper, fully or partially, from complying with its obligations under this regulation, including its obligations under Article 6(11) of that Regulation, on grounds of public security. Article 10 of Regulation (EU) 2022/1925 constitutes a valid legal basis for exempting Alphabet from its obligation to share Search Data with a specific undertaking applying for eligibility on grounds of public security. Such an exemption would be partial and targeted and would be without prejudice to Alphabet's obligation to comply with Article 6(11) of Regulation (EU) 2022/1925 with respect to any other undertaking applying for eligibility. While this power exists independent of the present Decision, the Commission considers it necessary to explicitly refer to this exemption procedure in case of a threat to public security.

(182) Article 10 of Regulation (EU) 2022/1925 provides that the Commission may take an exemption decision either on its own initiative or acting on a reasoned request from Alphabet.

(183) **Sixth and last,** Alphabet must not seek to use the eligibility assessment, transfer impact assessment, or reasoned request for an exemption under Article 10 of Regulation (EU) 2022/1925 to replace the independent verification mechanism

---

223 See responses to the public consultation of: [third party] – *"Our core concerns lie with the ambiguity in the procedure for data access. … risks for non-compliance exist in the procedural aspects…. The Commission places limitations on Alphabet in terms of the questions asked, which must not be unduly onerous or require divulging competitively sensitive information…. While prima facie appropriate, these remain high-level principles…."*, Doc ID […]; -[national public authority] *"…the proposed framework appears to leave a significant role to the gatekeeper in assessing eligibility. From an economic standpoint, this raises a clear risk of foreclosure through procedural or informational asymmetries, as access conditions could be used strategically to limit entry. In our view, eligibility criteria should therefore be interpreted broadly and applied under strict supervisory conditions, ensuring that the gatekeeper cannot exercise discretionary control over access. This is a necessary condition for the measure to effectively contribute to market contestability"*, Doc ID […]; [third party] – *"This framework raises concerns regarding governance and oversight. It assigns Alphabet a central operational role that includes decision-making authority over access…. Although procedural safeguards limit this discretion, Alphabet retains a degree of unilateral decision-making that may create issues in the event of disagreements with third-party OSEs"*, Doc ID […].

specified in section 4.4.4.2.4.1. The independent verification mechanism is intended to verify the implementation and ongoing compliance with the three assurance objectives identified in section 4.4.4.2.4.1.3, intended to ensure that the contractual measures specified at section 4.4.4.2.1, 4.4.4.2.2 and 4.4.4.2.3 are fully effective. Alphabet's eligibility assessments, transfer impact assessments and reasoned requests for an exemption under Article 10 of Regulation (EU) 2022/1925 must therefore be strictly limited to the matters specified at recitals (128) - (134).

(184) In this regard, the Commission notes that one response to the public consultation raised concerns that the eligibility criteria *"include no minimum threshold of demonstrated technical capacity to handle the dataset responsibly"*.[224] While third-party OSEs that meet the quantitative thresholds specified above are more likely than those that do not meet those thresholds to have the technical capacity to handle Search Data in a way that complies with the contractual measures specified at section 4.4.4.2, the specific assessment of whether a third-party OSE complies with those contractual measures is squarely within the scope of the independent verification mechanism specified in section 4.4.4.2.4.1. In particular, the first assurance objective requires the auditor to verify that a third-party OSE can demonstrate adequate resourcing for implementing and preserving anonymisation of the Search Data. In addition, the second and third assurance objectives specify that the auditor must verify that a third-party OSE has implemented effective measures to: ensure that Search Data is processed in compliance with the contractual obligations set out in this decision; and to protect the integrity and confidentiality of Search Data.

4.3. Measures relating to data scope and conditions of sharing

(185) This section presents the Commission's considerations on the specified measures and the reasons for them in relation to: the principle of parity as the guiding principle for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 (section 4.3.1); the scope of each of the data categories set out in Article 6(11) of the Regulation (section 4.3.2) and the conditions of data sharing (section 4.3.3). Each section provides an introduction, the specified measures (where applicable) and the Commission's assessment underpinning the measures.

4.3.1. Parity principle

4.3.1.1. Introduction

(186) The Commission considers that the guiding standard for data sharing under Article 6(11) of Regulation (EU) 2022/1925 is parity. This means, that subject to the anonymisation requirement and to what is technically feasible, Alphabet must share with third-party OSEs all ranking, query, click and view data on par with what it collects for the purpose of optimising OSE services. The limitation to this guiding principle, i.e., the requirement that personal data must be anonymised, is dealt with further in section 4.4 of this Decision.

(187) The objective of Article 6(11) of Regulation (EU) 2022/1925 is to remove an important barrier to third party OSEs' entry and expansion in terms of access to user data. Google Search has been the most popular OSE for over a decade, allowing it to accumulate an extensive amount of user data and using it to make search results responsive to user queries.[225] Article 6(11) of Regulation (EU) 2022/1925 seeks to make such data accessible to third-party OSEs, so that they can also optimise their OSE services and contest Google Search.

---

224 Response to the public consultation of [third party] Doc ID […].

225 Commission's Decision in AT.39740, Google Shopping, C(2017) 4444, para. 271 et seq.

(188) Section 4.3.1.2 provides the summary of gatekeeper's view, section 4.3.1.3 provides the Commission's assessment leading to the application of the general standard of parity to the data sharing measures in relation to the data scope and conditions of sharing.

4.3.1.2. The gatekeeper's view

(189) Alphabet argues that Article 6(11) of Regulation (EU) 2022/1925 does not impose a parity obligation for data sharing because (i) unlike other provisions of Regulation (EU) 2022/1925, such as Articles 6(5) and 6(7), Article 6(11) does not foresee a parity obligation;[226] (ii) the design of Article 6(11) of the Regulation contradicts the idea of parity, through the anonymisation requirement and through requiring the disclosure of only part of the data available to the gatekeeper,[227] and (iii) the legislator choice not to include horizontal interoperability obligations in the Regulation conflicts with a parity obligation.[228] More generally, Alphabet argues that the measures expropriate its intellectual property and innovation[229] as recipients would be able to copy the output of Alphabet's algorithms,[230] imitate Alphabet's algorithms[231] and freeride Alphabet's costly innovations and investments,[232] and that this expropriation conflicts with the DMA objectives.[233]

4.3.1.3. The Commission's assessment

(190) **First**, applying parity as the standard for sharing data which falls under the data categories listed in Article 6(11) of Regulation (EU) 2022/1925 is based on the text of the Article and its objectives. Therefore, applying the parity principle to the interpretation and operationalisation of Article 6(11) of Regulation (EU)2022/1925 ensures consistent and coherent interpretation of the Article in line with the objectives of the Article and the Regulation. ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 expressly prescribes the categories of data which the legislator considered to constitute an important barrier to entry when possessed by gatekeepers and therefore required Alphabet to specifically share them. Any partial or filtered access to data falling under these categories does not have a basis in Article 6(11) of Regulation (EU) 2022/1925. Nothing in Article 6(11) or recital 61 of Regulation (EU) 2022/1925 suggests any condition that could limit the scope of sharing the Search Data besides the needs of anonymisation. This is clarified by recital 61 of Regulation (EU) 2022/1925 which states that *"[a]ccess by gatekeepers to such ranking, query, click and view data constitutes an important barrier to entry and expansion, which undermines the contestability of online search engines. Gatekeepers should therefore be required to provide access […] to those ranking, query, click and view data."* Alphabet must therefore share all the "*ranking, query, click and view data*", which it collects and uses itself, rather than assess specific third parties' data shortages. ***In the second place***, the purpose of Article 6(11) of Regulation (EU) 2022/1925 is to remove the barrier to entry generated by gatekeepers' access to user data (i.e., the data asymmetries between gatekeepers and third-party OSEs), which implies that third parties should have access to the same Search Data as Alphabet has. Indeed, recital 61 of Regulation (EU) 2022/1925

226 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 332-340.
227 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 341-342.
228 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 343-347.
229 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 25-39.
230 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 40-50.
231 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 51-55.
232 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 56-64.
233 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 65-67.

considers gatekeepers' access to the Search Data as "*an important barrier to entry and expansion*", which should be removed by making this data, i.e., the same ranking, query, click and view data to which the gatekeeper has access, and which it collects for the purpose of optimising its OSE services, accessible to third parties, as laid down in Article 6(11) of Regulation (EU) 2022/1925.

(191) **Second**, unlike its alternatives, parity is an objective standard for data sharing, which does not require any assessment of the effectiveness of the data shared to allow contestability of OSE, nor does it require the assessment of third parties' individual data shortages and their ability to contest OSE. In this respect, Alphabet suggests determining data types subject to sharing based on the assessment of whether a specific piece of data can help third-party OSEs to fill the gap between the data they have and the more extensive data that Alphabet possesses due to its larger user base.[234] [235] However, setting a different standard that would require the gatekeeper to conduct such assessments in order to comply with its obligation pursuant to Article 6(11) of Regulation (EU) 2022/1925 is bound to lead to arbitrary, and likely less effective results. ***In the first place***, a standard requiring Alphabet to carry out a subjective assessment of third-party OSE's needs and abilities would allow it to make arbitrary choices, not necessarily supporting contestability given Alphabet's inherent incentives not to strengthen competitors. Such decisions might also be difficult to monitor and control. ***In the second place***, Alphabet is not in a position to carry out such assessments, in particular when Alphabet is required to make such assessments in order to comply with its obligation. The subjective nature of such assessments could eventually undermine effective and timely compliance, also affecting Alphabet's general obligation to demonstrate compliance under Article 8(1) of Regulation (EU) 2022/1925. ***In the third place***, determining the scope of Search Data based on the specific data disadvantage suffered by third-party OSEs, as suggested by Alphabet, is at odds with the language and objective of Article 6(11) of Regulation (EU) 2022/1925.[236] Such an assessment would go against the text of Article 6(11) of the Regulation and the objective of removing an important barrier to entry and expansion and allowing third-party OSEs to optimise their services and contest Google Search. ***In the fourth place***, setting a standard requiring an assessment of third parties' individual data shortages is also incompatible with the freedom that data recipients should have in deciding what data they want to use and how they want to use it among the data that Alphabet collects for the purpose of optimising OSE services. By contrast, the parity principle provides for an objective standard which allows Alphabet to clearly identify the data which it needs to share. ***In the fifth place***, a standard requiring an assessment of third parties' individual data shortages and their ability to contest OSE would introduce the requirement for the Commission to investigate on a case-by-case basis the effects on competition of a gatekeeper's given conduct, which the legislator explicitly rejected.[237]

---

234 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID […], question 2(b). Alphabet's reply to RFI 8 of 10 September 2025, Doc ID […], question 8.

235 While several respondent to the Public Consultation provided similar views, calling for a necessity assessment for the data sharing, (see, for example, submissions of [third party], Doc ID […]; [third party], Doc IDs […] and [third party], Doc ID […]), other supported the parity standard proposed by the Commission (see, for example, submissions of [third party], Doc ID […]; [market participant], Doc ID […]; [third party], Doc ID 2295; [market participant], Doc ID […]; [third party], Doc ID 2313-2314; [third party], Doc ID […], and [third party], Doc ID […]).

236 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID […], question 2(b). Alphabet's reply to RFI 8 of 10 September 2025, Doc ID […], question 8.

237 See recital 5 of Regulation (EU) 2022/1925: "[...] *enforcement occurs ex post and requires an extensive investigation of often very complex facts on a case by case basis.*"

(192) **Third**, Alphabet's claims concerning the illegality of the parity principle do not stand. ***In the first place*****,** the fact that the legislator did not explicitly specify parity as the relevant standard for data sharing under Article 6(11) of Regulation (EU) 2022/1925, while specifying a similar standard under other obligations set in the Regulation does not mean, as argued by Alphabet,[238] that the legislator sought to prevent the use of parity as the relevant standard for data sharing. Indeed, applying a consistent standard in the form of the parity principle, to guide the interpretation of Article 6(11) of the Regulation, ensures coherent interpretation, which is compliant with the objectives of that Article and the Regulation. If anything, the inclusion of a similar standard under other obligation of the Regulation should serve as confirmation to the appropriateness of the parity standard, and not as means to exclude it, as it demonstrates the legislators' endorsement of the principle to achieve the Regulation's objective. ***In the second place***, the anonymisation requirement set in Article 6(11) of the Regulation, and the fact that only a subset of the data available to the gatekeeper is subject to the disclosure obligation in Article 6(11) of the Regulation do not demonstrate an express choice by the legislator to negate the application of a parity principle to the interpretation of the Article, as argued by Alphabet.[239] **Firstly,** as explained in recital (190) of this Decision, the parity principle is based on the text of Article 6(11) of the Regulation and its objectives. **Secondly,** the parity principle does not expand the scope of the data disclosure, it rather serves to guide the interpretation of the various terms listed in Article 6(11) of the Regulation. The starting point of the interpretation process is the data categories listed in the Article. Subsequently, the parity principle serves to interpret the higher standard of the data which is then subject to the anonymisation requirement. There is therefore no contradiction between the parity principle and the language of the Article. **Thirdly,** the fact that Article 6(11) of the Regulation does not achieve full symmetry between the gatekeeper and third-party beneficiaries due to the need to protect personal data, cannot and should not be used as an argument to increase the asymmetry even further. The standard of parity is the appropriate standard and should be applied even if it is constrained by the anonymisation requirement. Not applying the parity principle altogether due to the anonymisation requirement would go against the objective of the Article, to remove barriers to entry and expansion generated through the asymmetric access of the gatekeeper to search user data. ***In the third place,*** regardless of the limited interpretive value of the non-paper referred to by Alphabet,[240] applying Article 6(11) of the Regulation in compliance with the parity principle does not generate "*horizontal interoperability*" nor any of the issues associated with it, as argued by Alphabet.[241] **Firstly,** the data sharing obligation pursuant to Article 6(11) of the Regulation, is entirely different from the horizontal interoperability described in the paper, even when a parity principle is applied to it. Unlike the horizontal interoperability between messenger services and social networks described in the non-paper Alphabet refers to, the data sharing obligation under Article 6(11) of the Regulation, even when interpreted pursuant to a parity principle, does not require Alphabet to make any changes to the way it operates its services and is disconnected from the relationships of the gatekeeper and beneficiaries with their users. In particular, the Article 6(11) data sharing obligation,

238 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 332-340.

239 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 341-342.

240 Alphabet refers to a working paper of the council of the European Union, containing a non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA. The paper clearly states that it "*does not represent nor has any bearing on the official position of the Commission*". See: https://www.iccl.ie/wp-content/uploads/2022/03/wk03135.en22.pdf page 5 .

241 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 343-347.

interpreted pursuant to a parity standard, does not require "*aligning or creating interfaces for a multitude of features that may not be exactly equivalent on both sides*",[242] nor any mirroring of the gatekeeper's and beneficiaries' service features.[243] It is therefore wrong to draw any conclusion based on a comparison between the horizontal interoperability between messenger services and social networks as described in the paper referred to by Alphabet and the data sharing obligation pursuant to Article 6(11) of the Regulation. **Secondly,** there is no risk that any of the issues listed in the non-paper as associated with horizontal interoperability between messenger services and social networks will arise due to the application of a parity standard. As rightfully stated by Alphabet, "*Art. 6(11) does not require Google to disclose all data that Google's search engine has at its disposal*".[244] Nor does applying a parity principle to its interpretation. Applying a parity principle to the interpretation of Article 6(11) will not achieve identity in the data accessible to Alphabet and third-party beneficiaries. Among others, this is because the data sharing applies to a limited list of data types and due to the anonymisation requirement which further limits the data to be shared.

(193) **Fourth,** the fact that [description of Alphabet's use of user data] does not justify the exclusion of such data from the data scope. [Description of Alphabet's internal systems].[245] However, the Commission considers that the display of general paid search results on the SERPs constitutes part of OSE services. [Description of Alphabet's use of user data]. As explained in more detail in section 4.3.2.2.3, paid search results are explicitly covered by Article 6(11) of Regulation (EU) 2022/1925 and form a substantial part of the SERPs. The definition of "*search results*" in Article 2, point (23), of Regulation (EU) 2022/1925 confirms that paid search results returned in response to a user query form part of the OSE services. The fact that the display of ads forms part of OSE services was further confirmed by the Commission in the Designation Decision,[246] and by Alphabet itself.[247] Finally,[Description of Alphabet's use of data].

(194) **Fifth**, applying the parity standard to data sharing under Article 6(11) of Regulation (EU) 2022/1925, and the specified measures more generally, will not expropriate Alphabet's intellectual property and innovation,[248] nor will they limit innovation.[249] Any reliance of the measures on Alphabet's effort or innovation do not go beyond what was intended for by the legislator.

(195) ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share ranking, query, click and view data which is *"generated by end users on its online search engines"* and does not require Alphabet to share any of its intellectual property. Recital 61 of Regulation (EU) 2022/1925 also clarifies that Alphabet's data sharing obligation centres on users and their interactions with Google Search,

---

242 See, the non-paper, under section 3, "heterogeneity of services".

243 *Ibid.*

244 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 341.

245 Alphabet's presentation to the European Commission on Search data & algorithm development dated 2 March 2026, Doc ID […].

246 Designation Decision, paragraphs 220-221

247 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID […], question 2.

248 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 25-67. Some respondents to the Public Consultation have made similar claims. See for example, submissions of [third party], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […].

249 Alphabet claims that sharing assets and information between competitors diminishes their incentives to innovate. See Alphabet's reply to RFI 1 of 23 November 2023, Tranche 2, Doc ID […], question 16, paragraph 4.

meaning that Alphabet should share "*information about what users searched for, and how they interacted with, the results with which they were provided*." As described in section 4.3.2, the measures specified by the Commission implement these principles and are limited to the data which enables eligible third party OSEs to understand user's interactions with Google Search. The measures do not require Alphabet to share its search infrastructure, technology or know-how. For example, they do not compel Alphabet to share its web index, search and ranking algorithms, ranking signals, LLMs, content of search modules or even minor in-house data, such as [description of Alphabet's internal processes and components].[250] The Commission notes that, while Alphabet argue generally that the measures "*expropriate Google's intellectual property and innovation*",[251] Alphabet does not specify, nor demonstrate, that sharing of search data pursuant to Article 6(11) of the Regulation and the measures concern any specific intellectual property protected by legal frameworks such as patents and copyrights, and that to substantiate its general claim, Alphabet rather refers to "intellectual effort".

(196) ***In the second place***, the objective of Article 6(11) of Regulation (EU) 2022/1925 is to foster innovation in the search services sector by enabling third-party undertakings to access the Search Data. As highlighted in recital 61, the sharing of such data is necessary to allow third-party undertakings to optimise their services and contest Google Search. The EU legislators decided that sharing of data owned by a gatekeeper such as Alphabet is required in light of very particular market circumstances, where the value of OSEs increases with the total number of users, and access to the Search Data constitutes a significant barrier to entry and expansion. As the Impact Assessment notes, granting third-party OSEs access to the Search Data should increase the level playing field between competitors, allowing them to optimise their services and compete more effectively with Google Search.[252] It follows that the sharing of the Search Data is deemed necessary to promote innovation by third parties.

(197) ***In the third place***, to the extent the sharing of ranking, query, click and view data with eligible third party OSEs make use of Alphabet's innovation (as argued by Alphabet),[253] this was the legislator's choice, and the measures do not require sharing any data that goes beyond the legislators' choice. **Firstly**, the legislator ordered the sharing of ranking, query, click and view data. The application of the parity principle only assists with identifying relevant data *within* ranking, query, click and view data, and does not extend the data beyond ranking, query, click and view data as ordered by the legislator. **Secondly**, the legislator's choice to order the sharing of data even if it requires data which is the result of Alphabet's investment, intellectual property and innovation, is demonstrated by the legislator's choice to order the sharing of view data and ranking data, both of which concern Alphabet's output. While the search data to be shared pursuant to Article 6(11) of Regulation (EU) 2022/1925 is *generated* by the users who input their queries and interact with the results, both

---

250 This conclusion is also supported by evidence from the United States of America ("**USA**"). The US Court arrived at this conclusion despite the fact that the dataset envisaged in its Opinion was far wider than the dataset envisaged in these Preliminary Findings. The dataset in the US Court's Opinion of 2 September 2025 in US v. Google included search index, click and query data as well as syndication. See Opinion of 2 September 2025, Doc ID […], page 162 – 163.

251 Alphabet's response to the Preliminary Findings, Doc ID [...], chapter 1, section I.

252 Commission Staff Working Document, Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector, COM (2020) 842 final, part 2, page 57.

253 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 25-67.

view and ranking data concern the output created by Alphabet and presented to the users. Recital 61 of the Regulation specifically refers to the sharing of data concerning "*the results with which* [the users] ***were provided***" [emphasis added]. Meaning, that the legislator chose to order the sharing of data generated and provided by Alphabet, and which goes beyond raw user data. **Thirdly**, the anonymisation requirement in Article 6(11) of the Regulation prevents the sharing of raw data and thus further demonstrates the legislator's choice in that respect.

(198) ***In the fourth place***, the measures do not allow recipients to copy the output of Alphabet's algorithms, imitate its algorithms nor free-ride Alphabet's efforts. **Firstly,** as discussed in recital (195) of this Decision, the measures do not require sharing of Alphabet's search infrastructure, technology or know-how, which can be readily used by third parties to generate the same search results as Google Search. **Secondly,** data granularity and completeness will be reduced due to anonymisation requirements, which will limit recipients' ability to copy or imitate Alphabet's algorithms and their output.[254] **Thirdly,** due to the anonymisation requirements and technical limitations, data will be shared with a significant latency of no less than seven days (see sections 4.3.3.2 and 4.4), thus preventing recipients from simply copying the output of Alphabet's algorithms as described by Alphabet.[255] **Fourthly**, third-party OSEs have explained that search data is inherently complex and difficult to learn from. For example, one market participant noted that "*Alphabet has thousands of different signals (features), most of which have complex and/or nuanced definitions*."[256] Even with access to the Search Data, they would need to add their own know-how to make the data usable, which would necessarily introduce divergence between their own search results and those of Google Search. One market participant explains that "*knowing how Alphabet combines its features into a score wouldn't directly help us combine our features into a score, because we have different sets of features.*"[257] Third parties confirm that, in line with the purpose of Article 6(11) of Regulation (EU) 2022/1925, they plan to use the Search Data to develop their own differentiated OSE services by crawling websites and adding them to their indexes, training query understanding technologies, and search and ranking algorithms.[258] **Fifthly,** the measures specifically prohibit the mere copying by recipients of search results directly from the dataset, see section 4.4.4.2.

(199) ***In the fifth place,*** the measures seek to ensure that eligible third party OSEs have sufficient incentive to innovate, rather than freeride Alphabet's efforts. **Firstly,** to be eligible to receive Search Data pursuant to Article 6(11) of Regulation (EU) 2022/1925, third party OSEs must demonstrate they provide OSE services as a genuine economic activity, i.e., third parties would have to have already made investments in OSE and provide OSE services for a certain duration. **Secondly**, the audit requirement set in the measures ensures that beneficiaries have credible plans demonstrating that they will use the data shared with them pursuant to Article 6(11)

254 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 40-55

255 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 40-50.

256 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 10. Also [market participant] states that it does not believe reverse engineering is possible. See [market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 7.

257 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 2.

258 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 1; [market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 1; [market participant]'s reply to RFI 1 of 18 November 2025, Tranche 1, Doc ID […], question 2; [market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 1; [market participant] reply to RFI 2 of 18 November 2025, Doc ID […], question 1; [market participant]'s presentation dated 12 February 2026, Doc ID […], page 15-16.

of the Regulation for the genuine development, improvement, or optimisation of their own OSE services (see section 4.4.4.2). **Thirdly,** limiting the duration of the data sharing to only five years (see section 4.3.3.4) also serves to ensure that eligible third party OSEs have sufficient incentives to use the data to develop their own search technologies, as solely copying Alphabet's output would be very short lived and thus an unsustainable business plan.

4.3.2. Data scope

(200) This section presents the Commission's considerations on the measures to be specified and the reasons for them in relation to each of query (section 4.3.2.1), view (section 4.3.2.2), click (section 4.3.2.3) and ranking data (section 4.3.2.4). Each section provides an introduction, the measures the Commission is specifying and the Commission's assessment underpinning these measures. All measures in this section are subject to anonymisation requirements which are dealt with in section 4.4. This means that the scope of data as described in the present section may not be fully shared by Alphabet or it may be shared at a less granular level to the extent that this is required to anonymise the data in line with the measures that are specified in section 4.4.

4.3.2.1. Query data

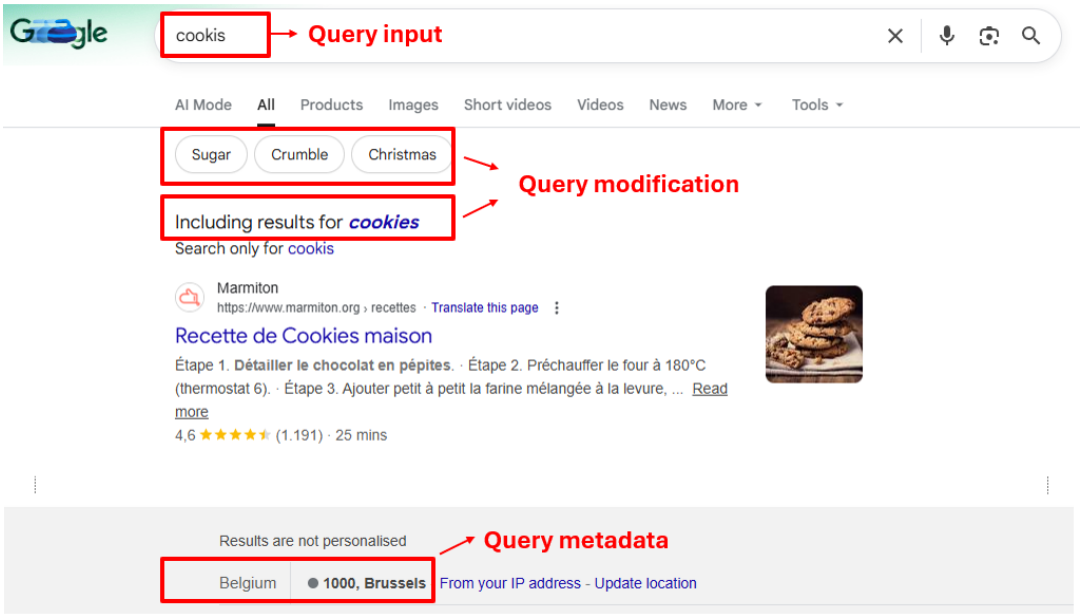
(201) This section presents the considerations of the Commission on the measures to be specified and the reasons for them in relation to query data. Section 4.3.2.1.1 provides a general introduction of query data, section 4.3.2.1.1.2 sets out the measures the Commission specifies in relation to query data, section 4.3.2.1.1.3 provides the summary of gatekeeper's view, section 4.3.2.1.1.4 provides the Commissions' assessment underpinning the measures, and sections 4.3.2.1.2 to 4.3.2.1.5 provide further assessment in relation to specific types of query data covered by the measures.

4.3.2.1.1. General

4.3.2.1.1.1. Introduction

(202) Users typically begin their interactions with OSEs by typing a query text in the OSE website or by speaking to an AI chatbot with search functionalities ("**query input**"). The OSE then processes this input. For example, it autocorrects spelling errors ("**query modification**") and adds relevant data about the user and query (e.g., user's location and query's language) ("**query metadata**") to understand the user intention behind the query to provide responsive search results (see Figure 4).

Figure 4: Illustration of query data on a Google Search SERP



Source: Own illustration

(203) Users also access OSEs through different access points, such as the website or a mobile application. Google Search receives queries through the following access points: the Google Search website, Google Search mobile application (including the Circle to Search feature),[259] Android Search widget, Google Lens application,[260] Google Assistant,[261] Gemini, AI Overviews, AI Mode, and text search on Android devices.[262]

(204) The Google Search Data provides search data from all search entry points discussed in the recital above, besides Google Assistant (partly), Gemini, AI Mode, Google Lens and Google Search's Circle to Search feature.[263]

(205) The Google Search Data includes the query text as entered by the user in line with Alphabet's interpretation that *"[q]uery data consists of the query text that users enter on Google*".[264]

(206) The Google Search Data also includes the query modified through several tools: the query shortcut chips, autocomplete function, entity results, query suggestions, "*see results about*" feature, autocorrect function and advanced search filters.[265]

(207) The Google Search Data does not distinguish between initial and modified queries, but includes all queries that produced a result page, except for automatically rewritten queries for which manually entered queries are included in the dataset even

259 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID […], question 6.
260 Alphabet's reply to RFI 11 of 12 November 2025, Tranche 1, Doc ID […], question 17.
261 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc […], question 6: [direct quote describing Alphabet's internal processes].
262 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID […], question 6.
263 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID […], question 7.
264 Alphabet's reply to RFI 4 of 15 May 2024, Doc ID […], question 18b.
265 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID […], question 5. Alphabet's reply to RFI 8 of 22 July 2025, Doc ID […], question 1. Alphabet also refers to the query box, but this is only a technical means of entering queries and is therefore not listed. For the definitions of each function see section 4.3.2.1.2.

though they do not produce a result page.[266] The Google Search Data does not include the content of query modifications displayed to the user either.[267]

(208) The Google Search Data also includes two query metadata attributes about the user and query: the location data at the country level[268] and the indicator of the device type (broken down into mobile/tablet and desktop).[269] The Google Search Data does not include any other query metadata.

(209) For the reasons listed in sections 4.3.2.1.1.4, 4.3.2.1.2.2, 4.3.2.1.3.2, 4.3.2.1.4.2 and 4.3.2.1.5.2 below the Commission considers specifying the query data which Alphabet must share under Article 6(11) of Regulation (EU) 2022/1925 in section 4.3.2.1.1.2.

4.3.2.1.1.2. Measures

(210) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, subject to anonymisation requirements, Alphabet must share with eligible third-party OSEs any query input entered by end users into Google Search on any access point, any modifications made by end users and Alphabet to this initial query, and any other metadata about the user and query, on par with the data collected by Alphabet for the purpose of optimising its OSE services.

(211) It follows that Alphabet must share with eligible third-party OSEs at least the following query data for each access point (e.g., Google Search website and browser omnibox on Chrome and third-party browsers, Google Search widget, Google Search application, Text Search on Android, Google Assistant, Google Lens and Circle to Search):

(a) Query input and modification data:

(1) Query input as entered by end users (the "**initial query**");

(2) Query as modified by end users and Alphabet (the "**modified query**"), including the modifications made through query shortcut chips, autocomplete function, entity results, query suggestions, "*see results about*" feature and autocorrect function;

(3) Content of query modifiers;

(4) Identifier of the type of query modification;

(b) Query metadata:

(1) User location;

(2) Query language; and

(3) User device, including mobiles, desktops and tablets.

---

266 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID […], question 4.

267 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID […], question 2(f).

268 Alphabet, Google European Search Dataset Licensing Program (February 2024), Doc ID […], page 3; Alphabet's reply to RFI of 28 February 2023, Table 1; Joint Feedback on Compliance with Article 6(11), DMA (Click-and-Query Data) of 5 December 2023, Doc ID […], page3.

269 Alphabet, Google European Search Dataset Licensing Program (February 2024), Doc ID […], page 3.

4.3.2.1.1.3. The gatekeeper's view

(212) In its response to the Preliminary Findings, Alphabet argues that the measures unjustifiably expand the scope of mandated data disclosures, based on alleged parity obligation and an over-reliance on the wishes of data recipients.[270]

(213) First, Alphabet submits that the Preliminary Findings demand disclosure of various data types that fall outside the scope of Article 6(11) of Regulation (EU) 2022/1925, including:

(a) queries generated by Gemini, which Alphabet considers to be a separate product that does not constitute an access point, and whose results are not displayed by Google Search;[271]

(b) queries posed by users to the Google Assistant and answered by the same, which are deemed to be outside the legal scope;[272]

(c) queries issued by users to search syndication partners, which are also considered to be outside the legal scope;[273]

(d) user contextual data (i.e., metadata) that are not categorised as query data, such as location data and device data.[274]

(214) Second, Alphabet submits that it does not collect some query data types proposed for disclosure by the Preliminary Findings as distinct data types within [Alphabet's internal components].[275]

4.3.2.1.1.4. The Commission's assessment

(215) As set out in section 4.3.2.1.1.2, the Commission considers specifying that Alphabet must share at least the following query data: query input, query modification and any other query metadata generated on any access points to Google Search.[276] The Commission provides below the reasons for which it considers specifying this measure.

(216) **First**, the term "*query data*" in Article 6(11) of Regulation (EU) 2022/1925 necessarily includes a broader set of information than the query text only.[277] If the EU legislature had intended to limit the scope of Article 6(11) of Regulation (EU) 2022/1925 to the query text, it would have used the term "*query text*" or "*query*". Instead, it chose the term *"query data"* which is a broader category, than the "*query text*", to which Alphabet wants to limit data sharing.[278] It is also broadly understood by the industry that query data include query text and various categories of query and user metadata.[279]

---

270 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 424.
271 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 459.
272 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 460.
273 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 463.
274 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 467.
275 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 486 and Annex 6, point 2 and 3, which concerns: modified queries, content of query modifiers, identifier of the type of query modification, indication of the method of query input and user's access point.
276 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.
277 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 471.
278 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 471.
279 See, for example, https://learn.microsoft.com/en-us/dynamics365/business-central/application/system/table/system.reflection.query-metadata, Doc ID [...], last accessed on 11 June

(217) **Second**, recital 61 of Regulation (EU) 2022/1925 describes query data broadly. It frames click, query, view and ranking data as the data intended to enable third-party OSEs to understand the entire chain of user interactions with the designated OSEs. recital 61 states that third-party OSEs should have access to gatekeepers' "*datasets containing information about what users searched for, and how they interacted with, the results with which they were provided. […] Gatekeepers should therefore be required to provide access […] to those […] query data […]*" (emphasis added). While Alphabet seeks to downplay the importance of recitals, it is undeniable that they provide more detail and context on how to interpret the operative text, and Article 6(11) DMA specifically, which uses the term "*query data*" that is further qualified in recital 61.[280]

(218) **Third**, recital 61 of Regulation (EU) 2022/1925 also makes clear that Article 6(11) of that Regulation requires Alphabet to share the Search Data to enable third-party OSEs to *"optimise their services"*. The term "*query data*" must therefore be interpreted also from this functional perspective and encompass the query data types which are necessary for understanding why a certain query generated certain results and thus allow the effective optimisation of OSE services. As shown in recital (236), third-party OSEs need to be able to follow all the modifications done to the initial user query and other data used to supplement it to be able to understand why given search results were matched with user's initial query to optimise their search technologies.

(219) **Fourth**, Article 6(11) of Regulation (EU) 2022/1925 requires the sharing of data "*generated by end users on [gatekeeper's] online search engines*", whereby the definition of OSE not only refers to the query text but also to "*other input*". Articles 2(6) of Regulation (EU) 2022/1925 cross-refers to Article 2(5) of Regulation (EU) 1150/2019 which defines an OSE as *"a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found"* (emphasis added). While Alphabet considers this term to only refer to "*the content of the query*",[281] the wording *"other input"* is broad and the input can also include all metadata about the user and query which complement the query.[282]

(220) **Fifth**, Alphabet itself seems to consider that query data includes metadata on queries and users entering them. While Alphabet contests this in its reply to Preliminary Findings,[283] this is inconsistent with its statements throughout the proceedings. Alphabet voluntarily offered to share user and query metadata – user location data and user device data – as part of query data to comply with Article 6(11) of Regulation (EU) 2022/1925,[284] which Alphabet itself acknowledges.[285] For example, Alphabet's compliance proposal from 2023 states that *"each data set will be organised on a "distinct query" basis. For example, the information for the query [Britney spears] in a particular geography and time period would be set out in one*

2026 and https://www.metaintegration.net/Products/MIMM/Help/user-guide/analyze/search-query-logs/?utm_source, Doc ID [...], last accessed on 11 June 2026 .

280 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 472.

281 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 473.

282 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 473.

283 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 467-476.

284 See Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], paragraphs 25-27.

285 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 474.

entry of the data set" (emphasis added).[286] According to Alphabet's compliance proposal from 2024:*"[t]he Dataset contains fields for: query string, country, device type*" (emphasis added).[287] Importantly, Alphabet uses the term "*query string*" (rather than "*query*") and follows it with user and query metadata, implying that it considers these data types as sub-types of query data. Alphabet also uses the terms, such as "*the query and associated metadata*" when replying to the Commission's various RFIs.[288]

(221) Alphabet's internal documents also demonstrate that [Alphabet's internal document describing Alphabet's views on query data][289] While Alphabet states that its internal documents [Alphabet's internal document describing Alphabet's views on query data],[290] [Alphabet's internal document describing Alphabet's views on query data].[291] [Alphabet's internal document describing Alphabet's views on query data].[292] [Alphabet's internal document describing Alphabet's views on query data][293] – [Alphabet's internal document describing Alphabet's views on query data].[294] The principle of parity therefore requires the sharing of all query metadata collected by Alphabet also with third-party OSEs.

(222) In addition, third-party OSEs report that the optimisation of OSEs requires access to several categories of query data. For example, market participants explain that initial queries are the most valuable signal of user intent, query modifications help understand intent evolution,[295] query's timing allows to know the state of the internet at the time the query was made[296] and user location helps OSEs decide on relevant search results.[297]

(223) **Sixth**, the Commission considers that Alphabet must share query data and other Search Data from any access point to Google Search. This at least includes Google Search website and browser omnibox on Chrome and third-party browsers, AI Overviews, AI Mode, Google Search widget, Google Search application, Text Search on Android, Google Assistant, Google Lens and Circle to Search.[298]

(224) ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 applies to the Google Search CPS, which covers search services provided through all access points to Google Search. The Designation Decision confirms that the Google Search CPS covers all search services that Google Search provides "*irrespective of the means through which users access such results (e.g. Google Search's website, app or*

---

286 Alphabet's submission "Art. 6(11) DMA: Update on Progress with our Compliance Solution" dated 19 April 2023, Doc ID [...], paragraph 3.

287 Alphabet's compliance report dated 6 March 2024, paragraph 107, available at https://transparencyreport.google.com/report-downloads, last accessed 11 June 2026. Note that Alphabet uses the term "*query string*" (rather than "*query*") and follows it with metadata, which implies that it considers these data types as sub-types of query data.

288 See, for example, Alphabet's reply to RFI 6 of 26 March 2025, Doc ID [...], question 2 and Alphabet's reply to RFI 11 of 12 November 2025, Doc ID [...], Tranche 2, question 9.

289 Alphabet's reply to RFI PO 12 of 13 November 2025, Annex 1.6, Doc ID [...], page 1.

290 Alphabet's reply to the Preliminary Findings paragraphs 476 and 477.

291 Alphabet's reply to RFI PO 12 of 13 November 2025, Annex 1.6, Doc ID [...], page 1. [Alphabet's internal document describing Alphabet's views on query data].

292 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.8, Doc ID [...], page 5.

293 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 1.

294 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.9, Doc ID [...], page 42.

295 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID […].

296 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID […], page 2.

297 [Market participants'] submission dated 4 June 2024, Doc ID […], page 18.

298 The text of the measure is repeated here for ease of reading. The binding text is provided in the the Annex to this Decision.

other)".[299] Alphabet agrees with this interpretation and confirms that Google Search Data provides search data from all search entry points with the exception of Google Assistant, Gemini, AI Mode, Google Lens and Circle to Search.[300]

(225) ***In the second place***, Alphabet must share the Search Data from Google Lens and Circle to Search. Alphabet states that "*searches via Lens are structured fundamentally differently from other searches because users input an image file rather than a query expressed with words. The search results returned for such searches are therefore different from those entered via other access points*."[301] Similarly, Alphabet reports that "*Circle to Search is an image search feature similar to Lens and like Lens does not have a query expressed in words associated with it*."[302] However, this is irrelevant from the standpoint of Regulation (EU) 2022/1925, which refers to queries as "*keyword, voice requests, phrases and other input*" as set out in Article 2(5) of Regulation 2019/1150.

(226) ***In the third place***, Alphabet must share the Search Data from AI Mode, AI Overviews and Google Assistant. The Commission also considers that Gemini is an access point to Google Search, but leaves the modalities of data sharing for the regulatory dialogue. In particular:

(a) With regard to AI Overviews and AI Mode, Alphabet already now includes the data from AI Overviews in the Google Search Dataset.[303] While the data from AI Mode has not been included yet[304] it should be also shared now based on the considerations in recital (c);

(b) With regard to Google Assistant, Alphabet also already now includes in the Google Search Dataset the queries and associated search data, which is generated if Google Assistant directs a user to Google Search, and the user clicks to trigger a search query in Google Search; and[305]

(c) With regard to Gemini, [direct quote describing Alphabet's internal system processes] [306] [direct quote describing Alphabet's internal system processes]. This conclusion is not called into question by Alphabet's claims that:

(1) [direct quote describing Alphabet's internal delineation]. .[307] The very concept of "*access points*" to Google Search relies on a premise that such access points are embedded in various products, such as a browser (e.g., Google Search omnibox), an operating system (e.g., text search on Android) or a separate application (e.g., Google Lense).

(2) [direct quote describing Alphabet's internal system processes]. .[308] As explained in recital (153), the Commission considers the grounding functionality of AI chatbots – be it the one of third-party AI chatbots or Gemini – constitutes an OSE functionality.

---

299 Designation Decision, paragraph 94.
300 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 7.
301 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 7.
302 Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], question 6.
303 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 6.
304 Alphabet's reply to RFI 3 of 11 February 2026, Annex Q3.12, Doc ID [...].
305 Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], question 6.
306 Alphabet's reply to RFI PO 10 of 23 March 2026, Doc ID [...]1739-1, question 3.
307 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 459(a).
308 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 459(b).

(3) "[direct quote describing Alphabet's internal system processes].[309] End users are the very source of queries [description of Alphabet's internal system processes]. .

(4) [Direct quote describing Alphabet's internal system processes].[310] [Direct quote describing Alphabet's internal system processes].

(d) Based on the above the Commission considers that, irrespective of their qualification in terms of type of service Google Assistant, Gemini, AI Mode and AI Overviews are all access points to Google Search and Alphabet is required to share the Search Data from these access points to comply with Article 6(11) of Regulation (EU) 2022/1925. Based on the information provided by Alphabet, the Commission notes that [Alphabet's internal system processes]. falling within the scope of Article 6(11) of Regulation (EU) 2022/1925 presents several specificities [Alphabet's internal system processes].[311] Given these specificities, the measures specified in the Decision should not apply as such to the sharing of Gemini's data. Alphabet should engage further with the Commission on the conditions and scope for the sharing of Gemini's data and adjustments needed to the measures set out in the Decision. For the avoidance of doubt, the data from AI Overviews, AI Mode and Google Assistant (in line with points (a) and (b) above) should be subject to the measures specified in this Decision.[312]

(227) ***In the fourth place***, the Decision clarifies that Alphabet is not requested to share the Search Data generated from syndication partners on third-party websites, contrary to Alphabet's representation.[313] In the Preliminary Findings, the Commission merely referred to Alphabet's own statement to third-party websites giving users access to Google Search[314] without assessing or bringing into scope this potential access point.[315]

(228) **Seventh**, the Commission considers that Alphabet must share query input no matter whether it is text, voice or image. Article 2(5) of Regulation (EU) 1150/2019 makes clear that the term "*query*" covers various forms of input as OSEs operate "*on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input*" (emphasis added). The Designation Decision also finds that Google Search CPS covers all queries, "*regardless of the input mechanism or format used, i.e. whether voice, text, or images*".[316] Alphabet also agrees with the sharing of text and voice queries, only refusing the sharing of image queries because the "*are structured fundamentally differently*".[317] The Commission considers this is irrelevant given the language of Article 2(5) of Regulation (EU) 1150/2019. That said, the

---

309 Alphabet's response to the to Preliminary Findings, Doc ID [...], paragraphs 459(c) and (d). [Alphabet's internal system processes], as claimed by Alphabet's response to the Preliminary Findings, paragraph 459(f).

310 Alphabet's response to the Preliminary Findings, Doc ID 2420-2[...], paragraph 459(e).

311 Alphabet's reply to RFI PO 13 of 12 May 2026, Doc ID [...], questions 1-6. [Alphabet's internal system processes], Doc ID [...].

312 Alphabet's reply to RFI PO 13 of 12 May 2026, Doc ID [...], questions 7 and 8.

313 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 463.

314 Preliminary Findings, paragraph 148 referring to Alphabet's reply to RFI 11 of 12 November 2025, Doc ID [...], Tranche 1, question 17.

315 Preliminary Findings do not refer to syndicated Google Search boxes on third-party websites anywhere else than in paragraph 148. See in particular, Preliminary Findings, Annex, which does not refer to such boxes.

316 Designation Decision, paragraph 94.

317 Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], question 8.

Commission does not discuss this further given anonymisation measures, which limit Search Data in relation to voice and image queries (see further section 4.4.4.1 below).

(229) **Eight,** Alphabet's claim [Alphabet's internal system processes] [318] is not relevant. The data recorded by Alphabet allows to infer this data [Alphabet's internal system processes and components]. Similarly, Alphabet's claim [Allphabet's internal system processes and components] is not relevant.[319] As discussed in section 4.3.1, what matters is that Alphabet collects such data for the purpose of optimising its OSE services.

4.3.2.1.2. Query input and modification

4.3.2.1.2.1. Introduction

(230) When a user enters a query input into an OSE, the OSE can either directly generate search results or it can modify the query input, for example, to correct spelling mistakes or to make the query more specific.

(231) Alphabet's query input and modification mechanisms are as follows:[320]

(a) Autocorrect function: Google Search may automatically modify the query a user has put in the search box if it detects, for example, a common misspelling (e.g., "*comdy*" modified to "*comedy*"). For the autocorrect function three scenarios are possible:

(1) The query is rewritten based on the corrected spelling and the results are based on the rewritten query, with a SERP displaying the message "*These are results for comedy. Search instead for comdy*";

(2) The query is rewritten, but both the original and the rewritten queries are used to generate search results, with a SERP displaying the message "*Including results for comdy. Search only for comedy.*";

(3) The query is not rewritten and a SERP is based on the wrong spelling, but Google Search displays the message "*Did you mean comedy?*" If the user clicks on it, the query is rewritten and the SERP is based on the corrected spelling;[321]

(b) Query shortcut chips: these enable users to issue a new query that consists of the user's original query plus the term of the query shortcut chip that the user selected. For example, if a user enters the query "*top movies*" and then selects the query shortcut chip for "*comedy*" a new query is issued for "*top comedy movies*";[322]

(c) Autocomplete function: enables users to add terms to their queries, but unlike shortcut chips, this happens while a user is typing out the initial query, rather than after the initial query is issued (e.g., for "*movi*", autocomplete can suggest "*movie*");[323]

---

318 [Alphabet's internal system processes and components]. Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 487.

319 See recital (214) .

320 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 5. Alphabet's reply to RFI 8 of 22 July 2025, Doc ID [...], question 1. Alphabet also refers to the query box, but this is only a technical means of entering queries and is therefore not listed.

321 Alphabet's email of 16 January 2026, Doc ID [...].

322 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 5.

323 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 5.

(d) Query suggestions: a SERP may include a block with query suggestions for related searches (e.g., "*People also search for*"). A click on a query suggestion will issue a new query with the query suggestion;[324]

(e) Entity results: these comprise results for real world entities (e.g., movies, places, artists) that Google Search may show in a response to the end user's initial query, but which also operate as query input features. For example, if a user searches for "*top comedy movies*" and then selects the entity result for the "*Movie A*" a new query is issued for the queries "*Movie A*" and a new result page for that query is shown;[325]

(f) "*See results about*" feature: a SERP may propose more specific searches for the user to complete when the user's query relates to an ambiguous entity which has multiple possible meanings. For example, if a user searches "*Harry Potter*", Google Search displays the message "*See results about*" with an option to click "*Harry Potter – Film series*" and "*Harry Potter – 2001 film*";[326] and

(g) Advanced search filters: this tool enables users to specify filter parameters for results, such as returning only pages that are in a specific language or that were published in a specific time frame.[327]

(232) The Google Search Data includes all the query modifications listed above.[328] For each type of query modification, the Google Search Data includes both the initial and modified query,[329] with the following exceptions:

(a) For the autocomplete function, the Google Search Data includes only the initial query.[330] Alphabet considers the autocomplete function not to modify a query, but to facilitate users entering a query by enabling them to complete the query without having to type it out;[331]

(b) For the advanced search filters, the Google Search Data:

(1) does not include the initial query but only the modified query for the filter parameters that are listed under the category "*find pages with*" and for the "*filetype*" filter; in these cases the modified query is composed of the initial query and filter parameters that get added to the initial query;[332] and

(2) does not include the modified query, but only the initial query for the following filters "*last update*", "*language*", "*region*" and "*user rights*".[333]

---

324 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 5. Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], question 2(b).

325 Alphabet's reply to RFI 5 of 6 September 2025, Doc ID [...], question 5.

326 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], question 2(c).

327 Alphabet's reply to RFI 8 of 22 July 2025, Doc ID [...], question 1. Alphabet does not list advanced search filters as query input or modifier mechanisms. However, the Commission's preliminary view is that they are also such mechanisms, as filter parameters are either added to the query issued or are otherwise taken into account together with the query to generate search results.

328 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], question 2(d).

329 Alphabet's reply to RFI 5 of 6 September 2025, Doc ID [...], question 5.

330 Alphabet's reply to RFI 5 of 6 September 2025, Doc ID [...], question 5.

331 Alphabet's reply to RFI 8 of 22 July 2024, Doc ID [...], question 3(c).

332 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], question 2(e).

333 Alphabet's reply to RFI 8 of 22 July 2025, Doc ID [...], question 2; Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 8(b).

(233) The Google Search Data does not systematically include both the initial query and its modification. Each of them is treated as an individual search event and needs to separately pass the anonymisation thresholds.[334] The Google Search Data does not indicate whether or how a query has been modified either.[335]

(234) In response to the Commission's Preliminary Findings, Alphabet did not express any concerns regarding the Commission's preliminary measures for query input and modification data.

4.3.2.1.2.2. The Commission's assessment

(235) As set out in section 4.3.2.1.1.2 the Commission specifies that Alphabet must share at least the following query input and modifier data: the initial query, modified query, content of query modifier and identifier of the type of query modification.[336] The Commission provides below reasons, additional to the reasons provided in section 4.3.2.1.1.4, for which it specifies this measure.

(236) **First**, third-party OSEs should receive all the ranking, query, click and view data needed to understand the entire chain of user interactions with the gatekeeping OSEs, including the journey from the initial query input to the final query. The concept of "*query*" is defined in Article 2(5) or Regulation (EU) 1150/2019 broadly and includes any form of query input. This concept should be interpreted in light of recital 61 of that Regulation, which provides that Alphabet should share "*information about <u>what users searched for, and how they interacted</u> with, the results with which they were provided*" (emphasis added).

(237) **Second**, the parity principle requires Alphabet to share the initial query, modified query, content of modifiers and type of query modification. As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. Alphabet confirms that it collects the initial query, modified query, content of query modifier and identifier of the type of query modification, of [description of Alphabet's internal system processes].[337] As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of OSEs, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(238) **Third**, third parties confirm that to optimise OSE services, they need to know what end users introduce into Google Search, how this query input is modified, what was the content of modifications proposed to users and what types of modifications are applied. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was: 5 for initial queries, 4 for modified queries and 3.2 for the identifier of the type of query modification (on

334 Alpahet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 4 (for query shortcut chips).

335 Alphabet's reply to RFI 11 of 12 November 2025, Tranche 2, Doc ID [...], question 9; Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], question 2(f).

336 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision..

337 [Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], Tranche 2, Annex Q13, raws no. 1-6. [Description of Alphabet's internal system processes and components]. . See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 15. [Description of Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 14.

the scale 1-5), showing that most of these data is "*essential*" or "*very important*".[338] One market participant explains the importance of each of these data types, saying that initial queries are the most valuable signal of user intent, query modifications are important to assess how ranking systems respond to different interpretations of user intent and to evaluate optimisation choices, and the flag of the type of modifier used provides contextual insight into query handling.[339] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

(239) **Fourth**, for most query modification types, the Google Search Data already now includes the initial and modified queries.[340] The measures therefore aim to clarify that Alphabet must share these data types systematically for all types of query modifications, including autocomplete, and enable data receivers to identify the content of query modifiers which were presented to the user and user was choosing from and the type of modification applied.

(240) With regard to the autocomplete function, the Commission considers that Alphabet should share the initial query before the autocomplete function is applied. Alphabet confirms that it internally registers the initial query.[341] [Description of Alphabet's internal system processes and components],[342] showing the importance of the initial query before it is autocompleted for the optimisation of Alphabet's OSE services. In addition, third parties confirm that they need the initial query before its autocompletion to optimise their OSE services.[343] As a result, Alphabet cannot treat the autocomplete function differently than other query modification tools and it must also provide the initial query to third-party OSEs in this case.

(241) With regard to the advanced search filters, the Commission considers that queries modified through advanced search filters are within the scope of Article 6(11) of Regulation (EU) 2022/1925.[344] However, it leaves this issue open, as in any event, the anonymisation measures require the removal of advanced search filters that were applied.

---

338 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participant's] reply to RFI 1 of 18 November 2025, Tranche 2, Doc ID [...], question 4; [market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 4; [market participant's] presentation, 26 January 2026, Doc ID [...], page 8. See also [market participant's] submission dated 17 November 2023, Doc ID [...], page 4; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 3; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], questions 1 and 4; Market participant's reply to RFI PO 1 of 17 February 2026, Doc ID [...], question 3.

339 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...].

340 Alphabet's reply to RFI 3 of 23 February 2024, Doc ID [...], question 1; Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 4.

341 Alphabet's reply to RFI PO 2 of 30 January 2026, Tranche 1, Doc ID [...], question 19(b).

342 [Description of Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 1.

343 [Market participant's] reply to RFI PO 1 of 28 January 2025, Annex 1, Doc ID [...], page 4. Agreed minutes of meeting with [market participant] , 26 January 2026, Doc ID [...], page 2.

344 [Description of Alphabet's internal system processes and components]. In addition, the advanced filters, including "*last update*", "*language*", "*region*" and "*usage rights*" filters, modify queries by making them more accurate. They also have an impact on search results by narrowing down search results. For Alphabet's view see Alphabet's reply to RFI 10 of 12 November 2025, Doc ID [...], question 8.

(242) With regard to sharing the content of query modifiers displayed to users in response to their query on which they click to modify the query, the Commission considers that this data type is in the scope of data sharing under Article 6(11) of Regulation (EU) 2022/1925. Alphabet itself collects the content of query modifiers [description of Alphabet's internal system processes and components].[345] In addition, third parties also confirm that they need the content of query modifiers to optimise their OSE services.[346] For example, the content of query modifiers can provide third-party OSEs insights into "*which suggested paths most effectively lead to successful results*", which can then be used for training and improving *"[a]utocomplete and suggestion ranking models, [q]uery rewriting systems; [and] [e]nd recognition models"*.[347] As a result, Alphabet must share the content of query modifiers clicked by users in response to their query as part of query data (for the content of query modifiers displayed but not clicked by users see section 4.3.2.2.5).

(243) With regard to sharing the type of query modification applied, the Commission considers that Alphabet must share the indicator of the query modification type applied. Alphabet itself collects the indicator of the type of modification applied to the query [description of Alphabet's internal system processes and components].[348] In addition, third parties confirm that they need the indicator of query modifications applied to optimise their OSE services.[349] One market participant explains that it "*needs to identify the type of modification applied (e.g., autocomplete, correction, etc.) in order to optimise query understanding, rewriting, and autocomplete systems*."[350] As a result, Alphabet must share the data which enables third parties to identify the type of query modification applied for Alphabet's own OSE services.

4.3.2.1.3. Location

4.3.2.1.3.1. Introduction

(244) Query input is often supplemented with other query metadata to make the query specific and search results more responsive to the implicit needs of end users. Location data is an important query metadata. For example, the query "*thai restaurants*" likely yields most helpful search results if it is supplemented with the information on user's location in a specific city.

(245) The Google Search Data includes the location data at a country-level basis.[351]

---

345 [Description of Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 15.

346 [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], questions 3-4; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4; [market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], question 3; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2-4; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4.

347 [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], questions 3-4.

348 [Description of Alphabet's internal system processes and components]. . See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 14. See also Alphabet's reply to RFI 10 of 12 November 2025, Annex Q1.2, Doc ID [...], page 3, [Alphabet's internal system processes and components]. .

349 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 1. [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 5.

350 [Market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], page 2. See also [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2.

351 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 6.

(246) In its response to the Preliminary Findings, Alphabet argues that location data falls outside the ordinary and natural scope of query data since location data is data about the user.[352] In that regard, Alphabet made general comments in relation to the sharing of any query and user metadata (see recital (213)(d)).[353]

4.3.2.1.3.2. The Commission's assessment

(247) As set out in section 4.3.2.1.1.2, the Commission specifies that Alphabet must share the detailed user location.[354] Below, the Commission provides reasons, additional to the reasons provided in section 4.3.2.1.1.4, for which it specifies this measure.

(248) **First**, location data is part of *"query data"* referred to in Article 6(11) of Regulation (EU) 2022/1925. As detailed in recitals (216)-(221), the concept of *"query data"* is broader than the query text and includes all data used to complement search queries and identify matching results. Article 2(5) of Regulation (EU) 1150/2019 also makes it clear that the query includes not only "*keyword, voice requests, phrases*" but also "*other input*" (emphasis added). While Alphabet argues that the location data is not "*query text*" or even "*query data*" but rather "*user data*",[355] recitals (216)-(221) demonstrate that location data is part of metadata which is used to supplement query and therefore also constitutes query metadata. While Alphabet contests this in its reply to Preliminary Findings,[356] this is inconsistent with its statements throughout the proceedings. Alphabet voluntarily offered to share user location data as part of query data to comply with Article 6(11) of Regulation (EU) 2022/1925 (see further recital (208)).

(249) **Second**, granular location data is a key search parameter that OSEs associate with user queries to provide relevant search results. Countries are not homogenous and for local queries, small changes in user location can alter results to a given query radically. This is especially evident in respect of local queries, which represent roughly one third of all Alphabet's queries.[357] For instance, a search for *"restaurants in my area"* may generate entirely different search results even between different neighbourhoods in the same city. In this example, the end user will not specify their location in the query text but will expect the OSE to use their precise location to tailor results for them.

(250) **Third**, the parity principle requires Alphabet to share the location data at the same level of granularity as Alphabet itself collects for the purpose of optimising its OSE services. Alphabet's internal documents demonstrate that [description of Alphabet's data collection methodology].[358] [description of Alphabet's data collection methodology].[359] [description of Alphabet's internal system processes and components].[360] [Description of Alphabet's internal system processes and components].[361] However, the question of the precise location data collected by

352 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 468.
353 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 474.
354 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.
355 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 468, 474.
356 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 467-476.
357 Alphabet's reply to RFI 1 of 28 November 2023, Doc ID [...], question 5.
358 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...]778, page 1.
359 Alphabet's reply to RFI 11 of 12 November 2025, Doc ID [...], question 14.
360 [URL link to an image displaying Alphabet's data collection methodology], Doc ID [...], last accessed on 13 April 2026.
361 [Description of Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9, Tranche 2, Annex Q13, raw no. 17, Doc ID [...]. See also Alphabet's reply to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...], page 1.

Alphabet for the purpose of optimising its OSE services can be left open since, for the purpose of anonymisation, this data will in any case be shared at a less granular level (see section 4.4.4.1).

(251) In addition, third parties confirm that they need granular location data to optimise their OSE services. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4.4 on a scale from 1-5, meaning that such data is on average "*essential*" for market participants.[362] Market participants explain that "*the results for the same query made in different locations can be very different. Accordingly, the ability to offer high-quality results in response to local searches is a relevant competitive factor for any OSE.*"[363] One of them further specifies that the location should be "*generalized into dynamically-sized cells that ensure each metadata+location combination represents at least 1,000 users … to improve [their] local search results*".[364] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

(252) Moreover, Alphabet's internal documents demonstrate that granular location data is crucial to provide relevant search results to users. For example, Alphabet's internal newsletter reports that [direct quote describing Alphabet's data collection methodology].[365] Alphabet's employee testifying in the US Google Search case also stated that [direct quote describing Alphabet's data collection methodology].[366]

4.3.2.1.4. Language

4.3.2.1.4.1. Introduction

(253) Users enter query input in various languages and expect to be delivered search results in the same language. Language is therefore an inherent part of OSE services.

(254) The Google Search Data does not provide a query language identifier. According to Alphabet, OSEs can infer or determine the language of the query from the query themselves.[367]

(255) In response to the Commission's Preliminary Findings, Alphabet did not express any concerns regarding the Commission's preliminary measures regarding the sharing of query language identifier.

---

362 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participant's] submission dated 5 March 2024, page 2, Doc ID [...]; [market participant's] reply to RFI PO 1, Annex 1, Doc ID [...], page 2.

363 [Market participants'] submission dated 4 June 2024, Doc ID [...], page 18.

364 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 2. See also [market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], Annex 1, page 2 and agreed minutes of meeting with [market participant] , 26 January 2026, Doc ID [...], page 2; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 5; [market participants'] submission dated 4 June 2024, Doc ID [...], page 39.

365 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.3, Doc ID [...], page 9.

366 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.11, Doc ID [...], Testimony of PAGE Pandurang Nayak in U.S. and Plaintiff States v. Google LLC vs [2020], Case No. 1:20-cv-03010 (D.D.C.), page 43.

367 Alphabet's reply to RFI 3 of 23 February 2024, Doc ID [...], question 1.

4.3.2.1.4.2. The Commission's assessment

(256) As set out in section 4.3.2.1.1.2, the Commission specifies that Alphabet must share the query language identifier in an explicit manner.[368] Below, the Commission provides reasons additional to the reasons provided in section 4.3.2.1.1.4, for which it specifies this measure.

(257) **First**, the query language identifier is part of *"query data"* referred to in Article 6(11) of Regulation (EU) 2022/1925. As detailed in recitals (216)-(221) the term *"query data"*, is broader than the query text and includes both the query text and other query metadata used to supplement the query when identifying search results.

(258) **Second**, the parity principle requires that third-party OSEs receive the same query data as Alphabet itself collects for the purpose of optimising its OSE services. In that context, the language is a key basis on which Google Search identifies and ranks search results.

(259) ***In the first place,*** Alphabet allows users to enter a variety of language identifiers to rank queries on its Google Search platform. These include the user's language settings[369] as well as language filters in advanced search results.[370]

(260) ***In the second place***, Alphabet's internal documents demonstrate that [description of Alphabet's internal system processes and components].[371] [Description of Alphabet's internal system processes and components].[372]

(261) In addition, third-party OSEs confirm that they need language identifiers to optimise their OSE services. Four market participants consider query language as a crucial element of search data shared under Article 6(11) of Regulation (EU) 2022/1925.[373] For example, one market participant explains that "*[r]elevance of results can be different for the same query depending on the region or language settings of the user, especially in countries like Belgium where multiple languages are spoken*."[374] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

4.3.2.1.5. Device type

4.3.2.1.5.1. Introduction

(262) Users enter search query input on different devices, including desktops, tablets and mobiles. Device information plays a role in delivering search results, as the presentation format and content varies by device. For instance, desktop searches may include additional search modules, whereas mobile searches often prioritise localised content.

---

368 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.

369 Alphabet's reply to RFI 8 of 10 September 2025, Doc ID [...], question 10.

370 Alphabet's reply RFI 8 of 10 September 2025, Doc ID [...], question 2.

371 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 18.

372 Response to RFI 10 of 12 November 2025, Annex Q14.8, Doc ID [...], page 9; Response to follow-up questions to RFI 10, Annex Q3, Doc ID [...], page 1; response to RFI 10 of 12 November 2025, Annex 5, Doc ID [...], page 2.

373 [Market participants'] submission dated 5 December 2023, Doc ID [...], page 1.

374 [Market participant's] submission dated 5 March 2024, Doc ID [...], page 3; see also [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 6.

(263) The Google Search Data includes the information on user device type.[375] It distinguishes between the queries made on a mobile device and queries made on a desktop computer.[376] However, within the mobile device category the Google Search Data does not distinguish between the queries made via tablets and queries made via mobiles.[377]

(264) In its response to the Preliminary Findings, Alphabet argues that device type data falls outside the scope of query data since device type data is user data.[378] In that regard, Alphabet made general comments in relation to the sharing of any query and user metadata (see recital (208)).[379]

4.3.2.1.5.2. The Commission's assessment

(265) As set out in section 4.3.2.1.1.2, the Commission specifies that Alphabet must share the user device type, broken down by mobile, tablet and desktop devices.[380] Below, the Commission provides reasons, additional to the reasons provided in section 4.3.2.1.1.4, for which it considers specifying this measure.

(266) **First**, the user device data is part of "*query data*" referred to in Article 6(11) of Regulation (EU) 2022/1925. As detailed in recitals (216)-(221), the concept of *"query data"* is broader than the query text and includes all data used to complement search queries. Article 2(5) of Regulation (EU) 1150/2019 also makes it clear that the query includes not only "*keyword, voice requests, phrases*" but also "*other input*" (emphasis added). While Alphabet argues that the device data is not "*query text*" or even "*query data*" but rather "*user data*",[381] recitals (216)-(221) demonstrate that device data is part of metadata which is used to supplement queries and therefore also constitutes query metadata. While Alphabet contests this in its reply to Preliminary Findings,[382] this is inconsistent with its statements throughout the proceedings. Alphabet voluntarily offered to share device data as part of query data to comply with Article 6(11) of Regulation (EU) 2022/1925 (see further recital (208)).

(267) **Second**, the granular device data is a parameter which OSEs use to match search results to a particular user query. Tablets and mobiles are not the same type of device, mainly due to their size. Tablets have bigger screens than mobiles but smaller than desktops, therefore the search results are displayed in a different way when comparing to the mobiles and desktops. Different devices have also different methods of input, which results in different click patterns. Furthermore, tablets are usually used at home for stationary activities, which can influence queries' intent.[383]

(268) **Third**, the parity principle requires Alphabet to share device type data, including on tablets. As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. Alphabet itself collects this data for the purpose of optimising its OSE

375 Alphabet's reply to RFI 6 of 26 March 2025, Doc ID [...], paragraph 2(d).

376 Alphabet's reply RFI 1 of 23 November 2023, Doc ID [...], question 2; Alphabet's reply to RFI 3 of 23 February 2024, Doc ID [...], question 1.

377 Alphabet's reply to RFI 4 of 15 May 2024, Doc ID [...], question 14.

378 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 468.

379 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 474.

380 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.

381 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 468, 474.

382 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 467-476.

383 [Market participant's] submission dated 5 March 2024, Doc ID [...], page 3; see also [market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 4.

services, and parity dictates that third parties should have the same level of access to it. For example, Alphabet collects and distinguishes between the data on mobiles, tablets and desktops [Alphabet's internal system processes and components].[384] As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(269) In addition, third-party OSEs require the data on devices, including for tablets, to optimise their OSE services. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 3.9 out of 5, meaning that for all market participants such data is "*very important*".[385] For example, one market participant reports that *"[c]lick and view data will be very different across desktop, tablet, and mobile, because these are different devices with different screen sizes, different user interfaces, different sets of modules shown, and a different number of organic results visible "above the fold" (without scrolling)."*[386] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

4.3.2.2. View data

(270) This section presents the considerations of the Commission on the measures to be specified and the reasons for them in relation to view data. Section 4.3.2.2.1.1 provides a general introduction of view data, section 4.3.2.2.1.2 sets out the measures specified in relation to view data, section 4.3.2.2.1.3 provides the summary of gatekeeper's view, section 4.3.2.2.1.4 provides the Commissions' assessment underpinning the measures, and sections 4.3.2.2.2 to 4.3.2.2.5 provide further assessment in relation to specific types of view data covered by the measures.

4.3.2.2.1. General

4.3.2.2.1.1. Introduction

(271) In response to a user's query, an OSE matches the query with its web index and identifies responsive organic search results, that are served to the users together with other types of search results within the meaning of Article 2(23) of Regulation (EU) 2022/1925. All these search results are then ranked on the SERPs within the meaning of Article 2(22) of Regulation (EU) 2022/1925. Google Search SERPs include a range of search results, which can be categorised in different ways (see Figure 5):

---

384 [Description of Alphabet's internal system processes and components]. See Alphabet's reply to RFI PO 9 of 5 March 2025, Tranche 2, Annex Q13, Doc ID [...], raw no. 19. See also Response to follow-up questions to Alphabet's reply to RFI 10 of 12 November 2025, Annex Q1.2, Doc ID [...], page 14.

385 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participants'] submission dated 5 December 2023, page 1, Doc ID [...]. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4.

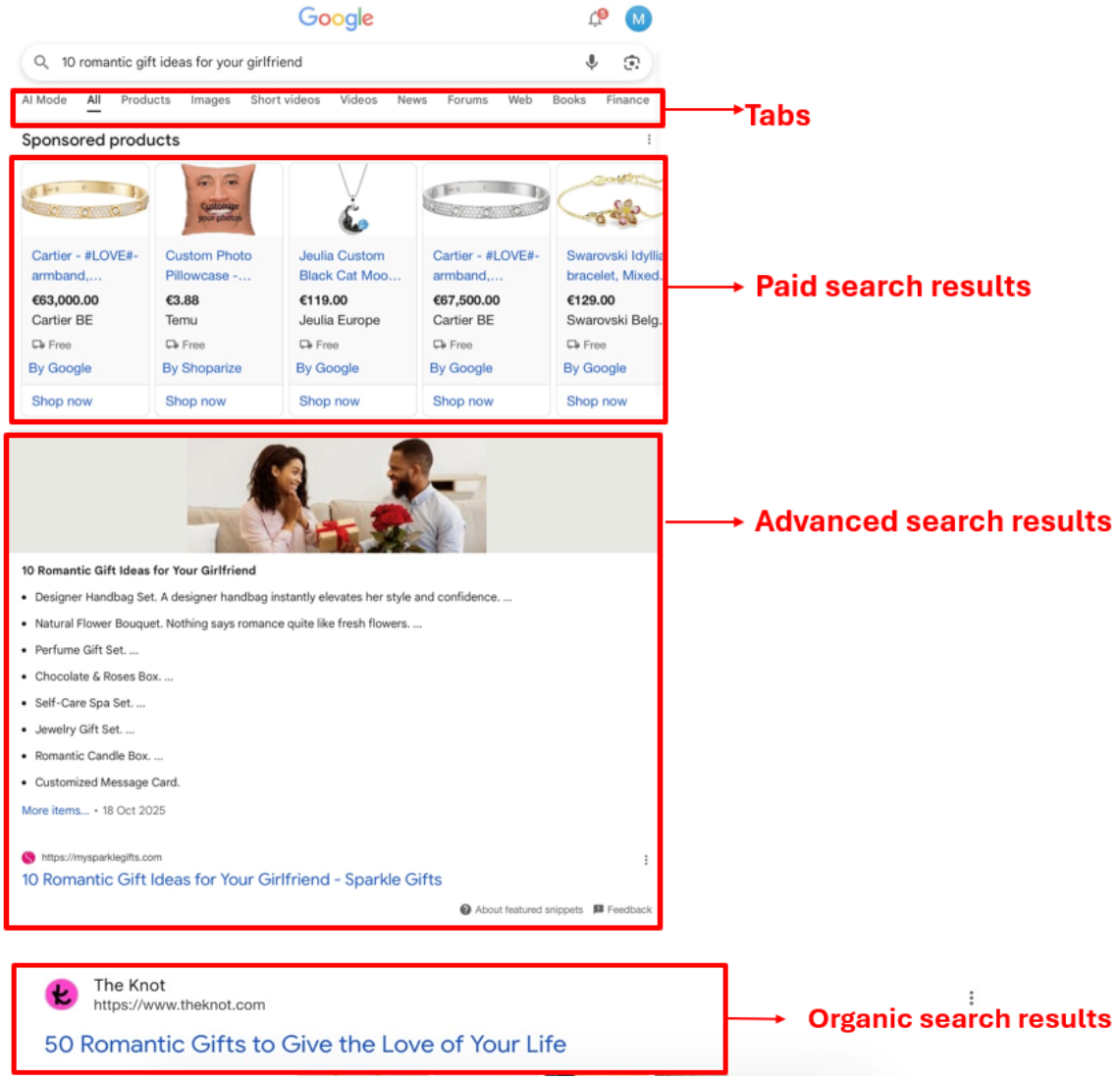
386 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4(c). See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4; [market participant's] reply to RFI PO 1, Annex 1, Doc ID [...], page 3; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 5.

(a) Depending on the topic, search results are organised in search "**tabs**" (e.g., "*Images*", "*Videos*").

(b) Depending on the remuneration, search results are either free or paid. Free results include organic search results, while paid results are ads or sponsored URLs for which a third party has paid to be ranked ("**ads**" or "**paid search results**").

(c) Depending on the format, search results can be the regular blue URLs that OSE identifies by crawling in principle all websites ("**organic search results**") or enhanced result formats which besides URLs, include graphical features and context ("**advanced search results**"). Advanced search results can also take the form of direct answers. Advanced search results can be free or paid search results. However, for clarity, this Decision includes in the advanced search results category only free search results. Paid advanced search results are not distinguished and are part of the paid search results category.

Figure 5: Illustration of view data on a Google Search SERP



Source: Own illustration

(272) The Google Search Data includes all the results displayed on the first SERP which were viewed by the end user, including organic, paid and advanced search.[387] While

387 Alphabet's reply to RFI 6 of 26 March 2025, Doc ID [...], paragraph 2f.

paid search results can be both organic and advanced search results, Alphabet classifies them as "*paid search results*", such that organic and advanced search results only include free search results.[388] This Decision follows this classification.

(273) For organic search results, the Google Search Data includes URLs and the identification that they are organic search results. The Google Search Data also includes both the main site URLs and "***associated [URLs]***", which are "*[URLs] that are part of an individual result and direct users to other pages of the referenced site that may also be of interest to the user*".[389]

(274) For paid and advanced search results, the Google Search Data does not include URLs, but only the indication that they are paid or advanced search results.[390] For advanced search results, the Google Search Data also includes an indication of the advanced result sub-type (e.g., Knowledge Panel, etc.).[391]

(275) The Google Search Data includes all search results, which were viewed by the end user, regardless of the tab, including *"Videos", "Short Videos", "News", "Forums", "Web", "Books"* and *"Finance",* with the exception of "*Images*", which are not included.[392] However, it does not contain an identifier of the tab type.[393]

(276) The Google Search Data includes the search results in all formats, such as text, image and video results. However, it does not contain an identifier of the format type.[394]

(277) For the reasons listed in sections 4.3.2.2.2.2, 4.3.2.2.3.2, 4.3.2.2.4.2 and 0, the Commission specifies the view data which Alphabet must share under Article 6(11) of Regulation (EU) 2022/1925 in section 4.3.2.2.1.2.

4.3.2.2.1.2. Measures

(278) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, subject to anonymisation requirements, Alphabet must share with eligible third-party OSEs any URLs and the description of visual elements which are displayed on SERPs, served to end users in response to their queries and are viewed by them (i.e., they generate an impression), no matter their type, format, structure or tab in which they are included on par with the data collected by Alphabet for the purpose of optimising its OSE services.

(279) It follows that Alphabet must share with eligible third-party OSEs at least the following view data:

(a) URLs:

(1) All URLs, regardless of the format of search result (e.g., photos, videos, text);

(2) All URLs, regardless of their structure (e.g., main URLs, associated URLs);

---

388 Alphabet's reply to RFI 1 of 28 November 2023, Doc ID [...], question 2.

389 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 1, Doc ID [...], question 13.

390 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 2; Alphabet's reply to RFI 6 of 26 March 2025, Doc ID [...], paragraph 2(f), (g).

391 Alphabet's reply to RFI PO 9 of 5 March 2026, Tranche 1, Doc ID [...], question 11(a).

392 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 12.

393 Alphabet's reply to RFI PO 9 of 5 March 2026, Tranche 1, Doc ID [...], question 10(b).

394 Alphabet's reply to RFI PO 9 of 5 March 2026, Tranche 1, Doc ID [...], question 9.

(3) All URLs for organic search results and advanced search results, and placeholders for paid search results, which are displayed in various search modules;

(4) All URLs, including from the following tabs: *"Videos", "Short Videos", "News", "Forums", "Web", "Books"* and "*Images*";

(b) URL identifiers:

(1) Identifier of the type of result format, including text, video and photo;

(2) Identifier of the place of result in the SERP's structure, including main and associated URLs;

(3) Identifier of the type of tab, including, for example "*Web", "Images", "Videos", "News"*;

(4) Identifier of the result type, including organic search results, identifier of paid search results, identifier of advanced search results, the latter including the identifier of sub-type, for example, *"Direct Answer", "Knowledge Panel*";

(c) Description of visual elements:

(1) The fact of displaying and the text included in query input areas, in query shortcut chips, entity results, query suggestions, "*see results about*" feature and similar, which are displayed on SERPs;

(2) The fact of displaying tabs on SERPs and their type; and

(3) The fact of displaying paid search modules and advanced search modules and their types, irrespective of whether such elements are displayed with or without an URL.

4.3.2.2.1.3. The gatekeeper's view

(280) In its response to the Preliminary Findings, Alphabet argues that the measures unjustifiably expand the scope of mandated data disclosures based on alleged parity obligation and an over-reliance on the wishes of data recipients.[395]

(281) First, Alphabet submits that the Preliminary Findings demand disclosure of the following data types that fall outside the scope of Article 6(11) of Regulation (EU) 2022/1925:

(a) the disclosure of URLs for advanced search results would reveal data pertaining to third-party services, they are outside of Google Search CPS and their sharing would be inconsistent with the DMA.100193 proceedings regarding Article 6(5) of Regulation (EU) 2022/1925 (on this see section 4.3.2.2.4);[396] and

(b) the proposed disclosure of URLs for paid search results would conflict with the Commission's Designation Decision, [description of Alphabet's internal system processes], and is regarded as disproportionate and as jeopardising anonymisation (on this see section 4.3.2.2.3). [397]

395 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 424.
396 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 477.
397 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 481-485.

(282) Second, Alphabet submits in the reply to the Preliminary Findings that [description of Alphabet's internal system processes and components].[398]

(283) Third, Alphabet submits in the reply to the revised specification measures that the measures on visual elements either duplicate the measures on query data or are not admissible as not covered in the Preliminary Findings.[399]

(284) Third, Alphabet raised questions on the actual scope of mandated data sharing in relation to visual elements.[400]

4.3.2.2.1.4. The Commission's assessment

(285) As set out in section 4.3.2.2.1.2, the Commission specifies that Alphabet must share all URLs and the description of visual elements which are displayed in SERPs, served to end users in response to their queries and are viewed by users regardless of their type, format, structure and tab, and the associated identifiers.[401] Below, the Commission provides reasons for which it specifies this measure.

(286) **First**, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share "*view data"*. This suggests that Article 6(11) of Regulation (EU) 2022/1925 does not require the sharing of all search results which were "*served*" by Google Search to users in response to their queries, but only those that were "*viewed*" by them. As explained in the following, this interpretation is supported by the industry practice and Alphabet itself.

(287) ***In the first place***, it is generally acknowledged by the industry that "*view data*" refers to the output of OSEs, namely "*search results*" (i.e., all the data provided in response to a query), which were "*viewed*" by the user (i.e., search results that generated an impression).[402]

(288) ***In the second place***, Alphabet considers that "*view data*" refers to search results, which were viewed by users. For example, Alphabet internally defines "*view data*" as "*information about what the user saw for Search results and relevant processing*" (emphasis added).[403] Alphabet also concludes that a "*view is the same as an impression*"[404]

(289) **Second**, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share all view data, including such as URLs regardless of their format (e.g., text, videos), structure (e.g., main and associated URLs), tab in which they are included (e.g.,

---

398 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 486 and Annex 6, point 2 and 3, which concerns: modified queries, content of query modifiers, identifier of the type of query modification, indication of the method of query input and user's access point.

399 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 63-69.

400 Alphabet's email dated 16 April 2026, Doc ID [...].

401 The text of the measure is repeated here for ease of reading. The binding text is provided in the the Annex to this Decision.

402 [Market participant's] submission dated 5 March 2024, Doc ID [...], footnote 4; [market participant's] response to RFI 2 of 18 November 2025, Doc ID [...], question 5; [market participant's] response to RFI 1 of 18 November 2025, Doc ID [...], question 5; [market participant's] response to RFI 1 of 18 November 2025, Tranche 2, Doc ID [...], question 5. Differently market participant's response to RFI PO 1 of 17 February 2026, Doc ID [...], question 4, where they require a minimum of 30 URLs per query. Also differently [market participant] , which states that "*What matters for [market participant] is receiving all URLs that were actually shown to the user*" (emphasis added). However also [market participant] implies that a given search result generated an impression "*The aim is to understand what users were exposed to on the results page, not to meet a fixed number threshold*.". See [market participant's] reply to RFI PO 1 of 28 January 2025, Doc ID [...], question 3.

403 Alphabet's reply to RFI 12 of 13 November 2025, Annex Q1.6, Doc ID [...], page 1.

404 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 2, Doc ID [...], question 15.

"Web", "Images" Videos", *"News"*) and type (e.g., organic, paid and advanced search results).[405] For clarity, Alphabet is also required to share URLs from the tab "*Images*", as its claim regarding technical difficulties with sharing such URLs is unsubstantiated (see further recital (291)).

(290) ***In the first place***, Article 2(23) of Regulation (EU) 2022/1925 makes clear that "*search results*" include any formats: "*'search results' means any information in any format, including textual, graphic, vocal or other outputs"* (emphasis added).

(291) ***In the second place***, Alphabet also considers that the view data covers all search results regardless of their format (e.g., text, videos), structure (e.g., main and associated URLs), tab (e.g., *"Videos", "News"*) or type (e.g., organic, paid search results), and covers them in the Google Search Data.[406] Alphabet only carves out "*Images*", justifying this by "*technical difficulties in adding data from this mode*".[407]

(292) ***In the third place***, third parties also confirm that they require search results no matter their format, structure, tab in which they are included or type for the optimisation of their OSE services. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4 on a scale from 1-5, meaning that such data is on average "*very important*" for market participants.[408] For example, one market participant noted that "*[f]ull visibility into which URLs were shown and in what form is essential to understanding relevance and ranking decisions*".[409]

(293) **Third**, the Commission considers that Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the indication of the link's format, structure, tab, and type (i.e., an organic search result, paid search result or advanced search result, the latter together with the type of advanced search result) for the reasons explained in recital (298).

(294) ***In the first place***, the term "*view data*" in Article 6(11) of Regulation (EU) 2022/1925 includes a broader set of information than the URL only. If the EU legislature had intended to limit the scope of Article 6(11) of Regulation (EU) 2022/1925 to URLs only, it would have used the term "*link*" or "*URL*". Instead, it chose the term *"view data",* which is a broader category.

(295) ***In the second place***, recital 61 of Regulation (EU) 2022/1925 also makes clear that Article 6(11) of that Regulation requires the gatekeeping OSEs to share search data to enable third-party OSEs to *"optimise their services."* The term "*view data*" should therefore be interpreted also from this functional perspective and encompass the data types which are necessary for third-party OSE providers to optimise their OSE

---

405 For the discussion on the types of search results, see sections 4.3.2.2.2, 4.3.2.2.3 and 4.3.2.2.4.

406 For the format and tab, see Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], questions 9 and 10a. For the structure, see Alphabet's reply to RFI 10 of 12 November 2025, Tranche 1, Doc ID [...], question 13. For the types of search results, see Alphabet's reply to RFI 1 of 28 November 2023, Tranche 1, Doc ID [...], question 2.

407 Alphabet's reply to RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], question 12.

408 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participants'] submission dated 5 December 2023, Doc ID [...], page 1. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4; [market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 5; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 3; [market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], Annex 1, page 3; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 8.

409 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 4.

services. As shown in recital (298), third parties need to be able to identify different types of search results included in the Search Data.

(296) ***In the third place***, Alphabet itself agrees with the interpretation that "*view data*" encompasses the indication of the type of search result. In particular, the Google Search Data already now includes the indication that search results are paid search results and advanced search results.[410] The measures therefore aim to clarify that Alphabet must share the indication of the format, structure, tab and type of search results systematically. This means that Alphabet must also share the indication of the URL's format, structure, tab, type, and sub-type of advanced search results (e.g., AI Overviews, Knowledge Panel, etc.).

(297) **Fourth**, the parity principle requires Alphabet to share the indication of the format, structure, tab and type of search results. Alphabet itself collects this data for the purpose of optimising OSEs, and parity dictates that third parties should have the same level of access to it. For example, Alphabet collects such data [description of Alphabet's internal system processes and components].[411] Which are according to Alphabet the [direct quote describing Alphabet's internal system components].[412] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(298) **Fifth**, third-party OSEs confirm that they need the identification of the format, structure, tab and type of search results to optimise their search technologies.[413] For example, a market participant reports that *"[f]ull destination page URLs, returned URLs, position of returned URLs and type of URLs (e.g., algo, advertisement) for both free and paid search are important for an online search engine's algorithms to "optimise", and specifically, to learn whether the URL is the most relevant for the user's search intent*" (emphasis added).[414] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

(299) **Sixth,** Alphabet's claim that [description of Alphabet's internal system processes and components].[415] As discussed in section 4.3.1, what matters is that Alphabet collects such data for the purpose of optimising its OSE services.

---

410 Alphabet's compliance report specifies that it shares "*results (exact URL for blue links, or type of other results, e.g., top text ad block or knowledge panel)*." See Alphabet's Compliance Report, paragraph 107.

411 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 28. [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 26. [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 25. [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 27.

412 Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], questions 16 and 19.

413 [Market participant's] submission dated 5 March 2024, Doc ID [...], page 2.

414 [Market participant's] submission dated 5 March 2024, Doc ID [...], page2.

415 See recital (282).

(300) Sections 4.3.2.2.2 to 4.3.2.2.5 below further discuss specific types of view data.

4.3.2.2.2. Organic search results

4.3.2.2.2.1. Introduction

(301) In response to a user's query, an OSE typically returns organic search results, ranked based on their relevance to answer the user's query, which link out to websites in which information related to the requested content can be found. In Google Search they usually appear on the left side of the first SERP in the form of "*blue links*" (i.e., URLs). For the purpose of this Decision, organic search results should be considered to only include free search results.

(302) The Google Search Data includes organic search results. Alphabet shares organic search URLs.[416]

(303) In response to the Commission's Preliminary Findings, Alphabet did not express any concerns regarding the Commission's preliminary measures regarding the sharing of organic search results.

4.3.2.2.2.2. The Commission's assessment

(304) As set out in section 4.3.2.2.1.2, the Commission considers specifying that Alphabet must share any organic search URLs and the description of visual elements which are displayed in SERPs, served to end users in response to their queries and are viewed by them (i.e., they generate an impression), no matter their type, format, structure or tab in which they are included.[417] Below, the Commission provides reasons, additional to the reasons provided in section 4.3.2.2.1.4, for which it considers specifying this measure.

(305) **First**, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share "*view data in relation to free [...] search generated by end users on its online search engine*". It is generally recognised that "*free search*" includes "*organic search results*", which are also called "*blue links*".

(306) ***In the first place***, Article 2(23) of Regulation (EU) 2022/1925 uses the term "*organic results*" to refer to the main body of results displayed by OSEs: "'*search results' means any information in any format, including [...] any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*" (emphasis added).

(307) ***In the second place***, the Designation Decision refers specifically to organic search results: "*all results or outputs that the Google Search CPS shows on its result pages, regardless of their format or type (thus including both organic results and the display of ads) ... constitute search results within the meaning of Regulation (EU) 2022/1925*" (emphasis added).

(308) ***In the third place***, Alphabet also considers that view data in relation to free search refer to organic search result URLs.[418] Accordingly, already now the Google Search Data includes organic search result URLs.[419]

(309) **Second**, the organic search result URLs are the heart of OSEs. The blue links are historically the first type of search results that were displayed by OSEs and until

---

416 Alphabet's reply to RFI 1 of 28 November 2023, Tranche 1, Doc ID [...], question 2.

417 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.

418 Designation Decision, paragraph 94.

419 Alphabet's reply to RFI 1 of 28 November 2023, Doc ID [...], question 2.

today they continue to constitute the backbone of SERPs. The organic search result URLs allow end users to navigate the web by connecting them to various websites related to their search query. In essence, the organic search result URLs are the primary mechanism by which OSEs help end users find and access relevant online content.

(310) **Third**, the parity principle requires Alphabet to share the organic search result URLs. Alphabet itself collects this data for the purpose of optimising its OSE services, and parity dictates that third parties should have the same level of access to it. For example, Alphabet collects organic search result URLs [Alphabet's internal system processes and components].[420] Organic search result URLs are also important for [description of Alphabet's internal system processes and components].[421] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(311) In addition, third-party OSEs also require organic search result URLs to optimise their OSE services.[422] The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4.9 on a scale from 1-5, meaning that such data is on average "*essential*" for market participants.[423] Market participants report that access to organic search results would help them overcome the challenges in crawling the web, such as the fact that many sites only allow established crawlers to enter their website, excluding their crawlers.[424] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

4.3.2.2.3. Paid search results

4.3.2.2.3.1. Introduction

(312) In response to an end user's query, an OSE may return paid search results (i.e., ad URLs or sponsored URLs), alongside organic search results. These search result

420 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 22.

421 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.8, Doc ID [...], page 4 et seq.

422 [Market participant's] submission dated June 2023, Doc ID [...], page 3, which refers to organic search result links as a "*mandatory*" OSE feature; [market participants'] submission dated 5 December 2023, Doc ID [...], page 1; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 3; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 3.

423 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participants's] submission dated 5 December 2023, Doc ID [...], page 1. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4.

424 [Market participant's] submission dated June 2023, Doc ID [...], page 3, which refers to organic search result links as a "*mandatory*" OSE feature; [market participant's] reply to RFI 1 of 18 November 2025, Tranche 1, Doc ID [...], question 2; agreed minutes of meeting with [market participant] of 21 May 2025, Doc ID [...], paragraphs 13-14; [market participant's] testimony in US Google Remedies Trial, Doc ID [...]and Doc ID [...].

URLs steer end users to advertised websites, which are determined based on the outcome of an advertisement auction. Paid search results usually appear above organic search results ("**top advertisement**") but can also appear among them ("**in-stream advertisement**"). Paid search results can also appear as part of advanced search results (e.g., paid placement in Alphabet's shopping comparison unit). For the purpose of this Decision, paid search results should be considered to include all paid results no matter whether they are placed alongside organic search results or whether they have the characteristics of advanced search results.

(313) The Google Search Data includes paid search results. However, Alphabet currently only discloses the information on the type of paid search displayed (i.e., text ad block or product ad block) without providing actual URLs of the viewed paid results.[425]

(314) In its response to Preliminary Findings, Alphabet argues that: (i) paid search results are not part of Google Search CPS,[426] (ii) [description of Alphabet's internal system processes], [427] (iii) the sharing of paid search result data violates the principle of proportionality,[428] and (iv) paid search result URLs disclosure would jeopardise anonymisation due to reidentification risks.[429]

4.3.2.2.3.2. The Commission's assessment

(315) As set out in section 4.3.2.2.1.2, the Commission specifies that Alphabet must share paid search results and visual content which are displayed in SERPs, served to end users in response to their queries and are viewed by them (i.e., they generate an impression), no matter their type, format, structure or tab in which they are included.[430] For anonymisation reasons, as explained section 4.4.4.1, paid search results can be shared without an URL (i.e., it is sufficient that the URL is replaced with a placeholder indicating that this is a paid search result). Below, the Commission provides reasons, additional to the reasons provided in section 4.3.2.2.1.4, as to why it specifies this measure.

(316) **First**, the text of Article 6(11) of Regulation (EU) 2022/1925 clearly covers paid search results. Article 6(11) of Regulation (EU) 2022/1925 is explicit that gatekeepers must share data in respect of both *"free and paid search"*. *"Paid search"* is an OSE industry term for advertising-driven search results. For example, one market participant markets their ads in the following way: "*Get your Ads served to an audience that is not on Google […] If your audience fits within what Ecosia offers, then it can be a considerably more cost-effective paid search option compared to it's competitors such as Google*" (emphasis added).[431] It is also a term that Alphabet itself uses. For instance, Alphabet states that "*[p]aid search results appear at the top of the SERP, and they feature a little green box with the word "Ad"*.[432]

(317) **Second**, Regulation (EU) 2022/1925 refers to *"paid search"* alongside "*free search*" across its various provisions, indicating that the legislators' intention was to cover both organic search results and paid search results as the OSE CPS. OSE services are

425 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 2; Alphabet's reply to RFI 3 of 23 February 2024, Doc ID [...], page 7.

426 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 482.

427 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 483.

428 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 484.

429 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 485.

430 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.

431 See https://www.purerdigital.com/ecosia-ads, Doc ID [...], last accessed on 13 April 2026.

432 See https://business.google.com/in/resources/articles/what-is-paid-search/, Doc ID [...], last accessed on 13 April 2026.

two-sided markets, one part being ads: "*[t]he web search market is an example of a two-sided market where internet users account for one side and the advertisers for the other*" (emphasis added).[433] In line with this, Article 6(11) of Regulation (EU) 2022/1925 refers to data sharing in relation to both "*free and paid search*". The definition of "*search results*" laid down in Article 2(23) of Regulation (EU) 2022/1925 also refers to "*a paid or an unpaid result*". It is clear therefore that the legislature intended the data sharing obligation in Article 6(11) of Regulation (EU) 2022/1925 to apply to ads that appear as part of search results.

(318) **Third**, the Commission has already confirmed that the display of search ads are within the scope of Google Search CPS and are therefore subject to Article 6(11) of Regulation (EU) 2022/1925. The Designation Decision states that *"[i]n line with Alphabet's view, the Commission further considers that the display of advertisements is also an integral part of the other service on which end users view the advertisement. It is common in the provision of online advertising services that end users are exposed to advertisements on other services. The fact that the display of an advertisement is part of Alphabet's online advertising CPS therefore does not exclude the fact that the act of displaying an advertisement is also part of Alphabet's other services, including CPSs on which the advertisement is displayed."*[434]

(319) Alphabet also agrees with the fact that the Google Search CPS covers "[direct quote describing Alphabet's internal system processes].[435] Alphabet's internal documents [direct quote describing Alphabet's internal definitions of data].[436] From that perspective, it is therefore inconsistent that Alphabet claims that paid search URLs are out of scope from the disclosure obligation, [description of Alphabet's internal system processes].[437]

(320) In any event, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share Search Data in relation to "*paid search generated by end users on its online search engine*" (emphasis added). The reference to the data "*on*" Google Search means that the legislator intended to cover all search results displayed on Google Search, no matter whether they are part of Google Search CPS or not. Article 2(23) of Regulation (EU) 2022/1925 refers to search results broadly, including search results which belong to the Google Search CPS or are distinct to it, including *"any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*". Article 6(11) of Regulation (EU) 2022/1925 relies on this definition, requiring Alphabet to share paid search results, [description of Alphabet's internal system processes].

(321) **Fourth**, the parity principle requires Alphabet to share paid search results. Alphabet itself collects paid search results for the purpose of optimising its OSE services, and parity dictates that third parties should have the same level of access to it. For example, Alphabet collects paid search result URLs [description of Alphabet's internal system processes and components].[438] While Alphabet claims that paid search result URLs are relevant only for its advertising services,[439] it also uses them

---

433 See https://www.researchgate.net/publication/227387683_Emergence_of_Global_Search_Engines_Trends_in_History_and_Competition, Doc ID [...], last accessed on 13 April 2026.

434 Designation Decision, paragraph 220.

435 Alphabet's reply to RFI 2 of 22 December 2023, Doc ID [...], question 9.

436 Alphabet's reply to RFI 12 of 13 November 2025, Annex Q1.6, Doc ID [...], page 1.

437 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 482.

438 Alphabet's reply to follow-ups to Tranche 2 responses to RFI 10 and 11 of 12 November 2025, Doc ID [...], question 4, [direct quote describing Alphabet's internal system processes]

439 Alphabet's reply to RFI 4 of 15 May 2024, Doc ID [...], Tranche 1, question 23.

to [description of Alphabet's internal system processes].[440] The fact that Alphabet decided to [description of Alphabet's internal systems], is irrelevant from the standpoint of Regulation (EU) 2022/1925, which applies irrespectively of gatekeepers' individual business models and follows the principle of technology neutrality (see, e.g., recital 14 of Regulation (EU) 2022/1925). What matters is that Alphabet optimises [description of Alphabet's internal system processes]. In any event, Alphabet collects paid search result URLs [description of Alphabet's internal system processes and components].[441] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(322) **Fifth**, Alphabet claims that it can only share the information on the type of paid search result displayed (i.e., ad block) without providing the actual underlying URLs because otherwise this would disclose Alphabet's and third parties' commercially sensitive information (i.e., identifying Alphabet's advertising customers,[442] getting insights into the performance of advertising keywords and successful advertising bidders).[443] The Commission does not engage with these claims as, in any case, the specified measures do not require Alphabet to share URLs related to paid search results for anonymisation purposes (see further section 4.4.4.1). The Commission eventually only requires Alphabet to disclose the information on the fact of displaying paid search modules and the type of paid search displayed (i.e., text ad block or product ad block) without providing the URLs of the paid search results, in line with Alphabet's initial proposal of sharing Google Search Data.[444] In any case the disclosure of paid search results was required by the legislator.[445]

(323) In addition, third parties confirm that access to paid search results is needed for the optimisation of their OSE services.[446] The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4.4 on a scale from 1-5, meaning that such data is on average "*essential*" for market participants.[447] Therefore, to ensure that third-party OSE "*can optimise their*

---

440 Alphabet's reply to follow-ups to Tranche 2 responses to RFI 10 and 11 of 12 November 2025, Doc ID [...], question 4, [direct quote describing Alphabet's internal system processes and components].

441 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 24.

442 Alphabet's reply to RFI 4 of 15 May 2024, Doc ID [...], question 23; Alphabet's reply to RFI 2 of 22 December 2023, Doc ID [...], questions 8 and 10; Alphabet's reply to RFI 4 of 15 May 2024, Tranche 1, Doc ID [...], question 23. See also Alphabet's reply to the Preliminary Findings, paragraphs 481-485.

443 Alphabet reply to RFI 4 of 15 May 2024, Doc ID [...], question 23; Alphabet's reply RFI 2 of 22 December 2023, Doc ID [...], questions 8 and 10; Alphabet's reply to RFI 1 of 23 November 2023, Tranche 2, Doc ID [...], question 17. See also Alphabet's reply to the Preliminary Findings, Doc ID [...], paragraphs 481-485.

444 See section 4.3.2.2.1.2.

445 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 396, 403 and 480.

446 See [market participants'] submission dated 5 December 2023, Doc ID [...], page 1. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4 and Market participant's reply to RFI PO 1 of 17 February 2026, Doc ID [...], question 5.

447 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market

services and contest the relevant core platform services", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

(324) Contrary to Alphabet's suggestion that paid search results would be used by third-party OSEs only to train ad algorithms,[448] market participants explain that paid search results are functionally similar to free search results and therefore used for the training of search algorithms.[449] For example, one market participant explains that "*on pages that displayed ads from expedia.com, we might infer travel intent for those queries and then study the relevancy of our organics and instant answers with the expectation that for the same/similar queries, we should have also shown local results*."[450]

(325) Moreover**,** market participants point out that paid search results are crucial for understanding user interaction patterns, as they contribute to providing the full SERP picture.[451] One market participant explains this based on a hockey related query "*odm*". It states that "*there can be a problem in query understanding if [market participant] has no information on what is behind the sponsored URL [which best reflects user's intent]. Take the example where user click data shows that 70% of users clicks on the sponsored result (which relates to hockey results but for which the URL is unknown to [market participant]), 10% on first organic link (hockey results, […]), and 20% on the second organic link ("wrong" "odm", [not related to hockey]). Here, the search engine may deduce that the second organic link (odm = original design manufacturer, 20% of clicks) is the more relevant abbreviation than the first organic link (odm = hockey results, 10% of clicks), even though this is incorrect*." (see Figure 6).

Figure 6: Paid search result URLs and query understanding

[…]

Source: [Market participant's] presentation dated 26 January 2026, Doc ID […], p. 6

(326) Last, the importance of paid search results for the regular training of search algorithms warrants particular emphasis, given that paid search results constitute a substantial part of the first SERP. Alphabet typically displays approx. 7 ads, three at the top and four at the bottom of SERP.[452] A large part of SERP (approx. 70% of the first page of results) and user's interactions with Google Search relate to ads.[453] Depriving third-party OSEs of paid search results would therefore substantially impede their ability to optimise their search engines and effectively compete with

---

participants'] submission dated 5 December 2023, Doc ID [...], page 1 and [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 4.

448 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 12.

449 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 6; [market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 6; [market participant's] reply to RFI 1 of 18 November 2025, Tranche 2, Doc ID [...], question 6; [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 4; market participant's reply to RFI PO 1 of 17 February 2026, Doc ID [...], question 5.

450 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 6.

451 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 3.

452 See https://support.google.com/google-ads/thread/6400917/how-many-ad-positions-are-there-in-google-serp-for-text-ads?hl=en#:~:text=Hi%2C-,It%20varies.,absolute%20you%20can%20count%20on, Doc ID [...], last accessed on 13 April 2026.

453 Ibidem.

Alphabet, thereby depriving Article 6(11) of Regulation (EU) 2022/1925 of its *effet utile*.[454]

4.3.2.2.4. Advanced search results

4.3.2.2.4.1. Introduction

(327) In response to an end user's query, an OSE may return advanced search results (i.e., search modules or panels), alongside organic and paid search results. These search results are enhanced result formats which besides URLs, include graphical features, context or direct answers. Advanced search results may include paid search results (e.g., paid placement in Alphabet's shopping comparison unit). However, for the purpose of this Decision, advanced search results should be considered to only include free search results.

(328) There are at least three types of advanced search results displayed on Google Search's SERPs, namely:

(a) "*Direct answers*", which include, for example, solutions to mathematical formulae, time of day, and dictionary results;

(b) "*Knowledge panels*", which include information on real-world entities, such as politicians, movie stars, authors, historical personalities, movies, games, books, historical events, mathematical and scientific concepts, astronomical objects, animals and local places; and

(c) "*Entity result blocks*", which identify results for different individual entities such as, politicians, philosophers, planets, animals, artists, music, movies, books and events.[455]

(329) The Google Search Data includes advanced search results. However, Alphabet current only discloses the information on the type of advanced search results displayed without providing actual URLs or other content shown in advanced results blocks.[456]

(330) In its response to the Preliminary Findings, Alphabet argues that (i) URL data from advanced search modules which are subject to the DMA.100193 proceedings regarding Article 6(5) of Regulation (EU) 2022/1925 are not results of Google Search,[457] and (ii) the disclosure of URLs for advanced results would reveal data pertaining to third-party services.[458]

4.3.2.2.4.2. The Commission's assessment

(331) As set out in section 4.3.2.2.1.2, the Commission specifies that Alphabet must share any advanced search result URLs and the description of visual elements which are displayed in SERPs, served to end users in response to their queries and are viewed by them (i.e., they generate an impression), no matter their type, format, structure or tab in which they are included.[459] Below, the Commission provides reasons,

---

454 [Market participant's] submission dated 5 March 2024, Doc ID [...], page 2. See also [market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 3.

455 Alphabet's reply to RFI 2 of 22 December 2023, Doc ID [...], question 7.

456 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 2; Alphabet's reply to RFI 3 of 23 February 2024, Doc ID [...], question 1.

457 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 432, 477-479.

458 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 480.

459 The text of the measure is repeated here for ease of reading. The binding text is provided in the Annex to this Decision.

additional to the reasons provided in section 4.3.2.2.1.4, for which it specifies this measure.

(332) **First**, Article 6(11) of Regulation (EU) 2022/1925 makes no distinction between the organic search results and advanced search results, but refers to them jointly as "*view data*" in relation to "*free search*". Accordingly, Alphabet is required to share *"view data"* in respect of advanced search on the same terms as it is required to share such data in respect of organic search results, which means the sharing of actual URLs.

(333) **Second**, contrary to what Alphabet suggests,[460] Regulation (EU) 2022/1925 does not distinguish between *"results content"* and *"results"*. Alphabet argues that advanced search results are "*results content*" rather than regular "*results*" and therefore do not fall into any of the click, query, ranking and view data covered by Article 6(11) of Regulation (EU) 2022/1925.[461] However, such distinction has no basis in Regulation (EU) 2022/1925. Article 2(23) of Regulation (EU) 2022/1925 explicitly states that *"search result"* shared as "*view data*", include advanced search results and such results are framed broadly. Namely, Article 2(23) of Regulation (EU) 2022/1925 defines "*search results*" to include *"any information in any format […] returned in response to, and related to, a search query, irrespective of whether the information returned is […] a direct answer or any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them"* (emphasis added). Advanced search results are results which are returned in response to search queries as either a direct answer or as information offered in connection with the organic results and accordingly meet the definition of *"search results"* under Article 2(23) of Regulation (EU) 2022/1925.

(334) **Third**, Alphabet itself implicitly agrees with the interpretation that advanced search results are covered by Article 6(11) of Regulation (EU) 2022/1925. The Google Search Data already now includes view data in relation to advanced search results – it includes the indication that a search result is an advanced search result.[462] Alphabet's internal documents [direct quote describing Alphabet's internal definition of data].[463]

(335) At the same time, Alphabet states that the disclosure of URLs for advanced search results oversteps the boundaries of Article 6(11) of Regulation (EU) 2022/1925 "*on the Commission's own case in Art. 6(5) Preliminary Findings, [which states that they] belong to separate services*".[464] The Commission considers that Article 6(11) of Regulation (EU) 2022/1925 does not support this interpretation. Article 6(11) of Regulation (EU) 2022/1925 lays down that Alphabet must share any data in relation to "*free and paid search generated by end users on its online search engine*". The reference to the data "*on*" Google Search means that the legislator intended to cover all search results displayed on Google Search, no matter whether they are part of Google Search CPS or not. Article 2(23) of Regulation (EU) 2022/1925 refers to search results broadly, including search results which belong to the Google Search CPS or are distinct to it, including *"any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*". Article 6(11) of Regulation (EU) 2022/1925 relies on this

460 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 10.

461 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 10.

462 Alphabet's compliance report specifies that it shares "*results (exact URL for blue links, or type of other results, e.g., top text ad block or knowledge panel)*." See Alphabet's Compliance Report, paragraph 107. See also Alphabet's reply to RFI 8 of 22 July 2025, Doc ID [...], question 6.

463 Alphabet's reply to RFI 12 of 13 November 2025, Annex Q1.6, Doc ID [...], page 1.

464 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 477-479.

definition, requiring Alphabet to share paid search results, which are generated by Alphabet's online advertising services CPS. In the same vein, the fact that some search results form part of a distinct service to the Google Search CPS is not an obstacle to their sharing also in relation to advanced search result URLs.

(336) **Fourth**, the parity principle requires Alphabet to share advanced search result URLs. Alphabet itself collects them for the purpose of optimising its OSE services. For example, Alphabet confirms that it collects advanced search [description of Alphabet's internal system processes and components][465] [Alphabet's internal system components].[466] [Alphabet's internal system components].[467] [Description of Alphabet's internal system processes and components].[468] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(337) In addition, Alphabet's internal documents demonstrate that advanced search result URLs are important for Alphabet for several reasons.

(338) ***In the first place***, Alphabet's internal documents demonstrate that the knowledge of advanced search result URLs is crucial for Alphabet to have a correct understanding of user interaction on SERPs:

(a) As Alphabet itself puts [direct quote describing Alphabet's internal system processes and components];[469]

(b) Alphabet's internal documents show that Alphabet put a lot of effort into enabling [direct quote describing Alphabet's internal system processes and components];[470] and

(c) Alphabet's internal documents also report that [direct quote describing Alphabet's internal system processes and components][471] and [direct quote describing Alphabet's internal system processes and components].[472]

(339) ***In the second place***, Alphabet's internal documents demonstrate that [description of Alphabet's internal system processes and components]:

(a) The illustration below from Alphabet's internal newsletter shows that [description of Alphabet's internal system processes]:

---

465 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 23. See also Alphabet's reply to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...], page 1.

466 For example, Tangram [Alphabet's internal system components]. See Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 71; Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 4; Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.9, Doc ID [...], page 62.

467 See footnote 465. See Alphabet's reply to follow-up questions to its response to RFI 10 of 12 November 2025, Doc ID [...], Annex Q.1, page 2, 49.

468 See footnote 466.

469 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.9, Doc ID [...], page 6.

470 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.13, Doc ID, [...], page 1.

471 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.13, Doc ID [...], page 1.

472 Alphabet's reply to RFI 12 of 13 November, Annex Q1.12, Doc ID [...].

Figure 7: Search results covered by [Alphabet's internal system component]

[Image displaying the result of Alphabet's internal system processes]

Source: Response to RFI 10 of 12 November 2025, Annex Q5, Doc ID […], p. 4.

(b) Alphabet's internal documents also show that the advanced search results URLs influence which organic search result URLs are displayed to the user: "*[i]f people query about the relation of a famous person, Knowledge Graph tells traditional search the name of the relation and the famous person, to improve search results*";[473]

(c) [Direct quote and description of Alphabet's internal system processes and components]."[474] [Direct quote describing Alphabet's internal system processes and components].[475]

Figure 8: [Image displaying the result of Alphabet's internal system processes]

[…]

Source: Response to RFI 10 of 12 November 2025, Annex Q5, Doc ID […], p. 8.

(340) ***In the third place***, Alphabet's internal documents [description of Alphabet's internal system processes and components]:

(a) [Direct quote describing Alphabet's internal system processes and components];[476]

(b) [Direct quote describing Alphabet's internal system processes and components];[477]

(c) [Direct quote describing Alphabet's internal system processes and components];[478] and

(d) [Direct quote describing Alphabet's internal system processes and components].[479]

(341) In addition, third parties confirm that access to advanced search URLs is needed for the optimisation of their OSE services. Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data sharing obligation specified in Article 6(11) of Regulation (EU) 2022/1925. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4.4 on a scale from 1-5, meaning that such data is on average "*essential*" for market participants.[480]

(342) Contrary to Alphabet's claim that advanced search result URLs will not enable third-party OSE providers to develop their own search algorithms,[481] market participants explain that such URLs are functionally similar to organic search result URLs and

473 Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 4.
474 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...], page 8.
475 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...], page 9.
476 Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 71.
477 Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 4.
478 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.9, Doc ID [...], page 62.
479 Alphabet's reply to RFI 11 of 13 November 2025, Annex Q1.16, Doc ID [...], page 72.
480 See also [market participants'] submission dated 5 December 2023, Doc ID [...], page 1. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], Question 4; Market participant's reply to RFI PO 1 of 17 February 2026, Doc ID [...], question 8.
481 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 10.

are therefore used for the optimisation of OSE services.[482] In particular, advanced search result URLs seek to identify information that is responsive to the user's query and are therefore functionally similar to organic search result URLs, often replacing the traditional blue links.[483] Third-party OSEs could therefore use advanced search result URLs to also identify responsive organic search result URLs. For example, one market participant states that advanced search results URLs, similarly to organic search result URLs, allow for *"[u]nderstanding what a user clicks on in response to a query, whether it be a static link or a dynamic answer block, is critical to machine learning to understand user intent – which in turn feeds directly into improving relevance and ranking."*[484] It adds that it *"does not believe it is justified to supress URLs and clicks just because Google decides to present them in a unique frame."*[485]

(343) Market participants also point out that advanced search result URLs are crucial for understanding use interaction patterns, as they contribute to providing the full SERP picture. For example, one market participant states that *"[a]dvanced search results often contain information and URLs that are important for understanding overall user behavior (reasons for not clicking on organic results)"*.[486] Similarly, another market participant explains that *"[a]dvanced modules (e.g., Top Stories, Knowledge, answers) materially affect user choice and must include URL-level detail to be useful"*.[487]

(344) In addition, market participants explain that advanced search result URLs could help them decide whether to surface advanced search modules and improve their relevance, emphasising that such modules are increasingly important when providing search services. Market participants explain the following:

(a) One market participant reports that "*search engine needs to provide high-quality search features in addition to organic web links, such as instant answers*",[488] given "*the increasing use of instant answers [following] the rise of smartphones, which now generate the majority of online searches*."[489] To that end, the market participant states that it needs advanced search result URLs such as "*Definitions", "Wikipedia references", "Quick answers", "AI chatbots", "Question/Answer references", "Recipes*";[490]

(b) A second market participant explains its general perspective that *"advanced search URL links can help optimise an OSE. Without visibility into these advanced result formats, an Alphabet rival's optimisation process would be biased toward "blue-link-only" results and would fail to accurately interpret user behaviour on pages where a substantial share of user satisfaction occurs without any clicks*";[491]

(c) A third market participant confirms that "*SERP composition data including displayed modules, their position, and the data used would enable us to*

---

482 [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 5; market participant's reply to RFI PO 1 of 17 February 2026, Doc ID [...], question 8.

483 Agreed minutes of meeting with [market participant] , 15 February 2024, Doc ID [...].

484 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 9.

485 [Market participant's] submission dated 12 February 2024, Doc ID [...], page 4.

486 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 3.

487 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 4.

488 [Market participant's] submission dated June 2023, Doc ID [...], page 1. See also [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 9.

489 [Market participant's] submission dated June 2023, Doc ID [...], page 4.

490 [Market participant's] submission dated June 2023, page 3, Doc ID [...].

491 [Market participant's] reply to RFI 1 of 18 November 2025, Tranche 2, Question 9, page 8, Doc ID [...].

improve the overall search experience. For our query understanding component, the data would enable us to train and display models of intent, SERP composition such as navigation bar displaying verticals (also when to trigger a module and where to position it in the SERP), as well as an entity extraction service."[492]

(345) **Fifth**, the importance of advanced search result URLs for OSE optimisation warrants particular emphasis given that such URLs constitute a substantial and highly prominent part of the first SERP, normally appearing at the top (see Figure 9 below). Depriving third-party OSEs of advanced search URLs would therefore substantially impede their ability to optimise their OSE services and effectively compete with Alphabet, thereby depriving Article 6(11) of Regulation (EU) 2022/1925 of its *effet utile*.[493]

Figure 9: Advanced search results on a Google Search SERP

[…]

Source: [Market participant's] presentation, 26 January 2026, Doc ID […], p. 14

(346) **Sixth**, the Commission considers that the risk of third parties violating Alphabet's intellectual property rights by copying Google Search is relatively low.[494] The measures which the Commission specifies do not oblige Alphabet to share the content of advanced search modules, but merely URLs to which users are directed. This addresses Alphabet's concern that the sharing of content could enable third-party OSEs to simply copy it into their SERPs, violating copyrights of third parties that license data to Alphabet and free riding on Alphabet's efforts and investments to assemble information for advanced search blocks.[495]

(347) Contrary to Alphabet's claim, a mere disclosure of URLs is also unlikely to appropriate inventory information of third-party websites, by revealing, e.g., what products, hotel rooms, flights, or local businesses the websites in question have in their inventory, and how well a particular product is doing[496] and, in any case, the disclosure of search results was required by the legislator.[497] In the first place, as explained above, Article 6(11) of Regulation (EU)2022/1925 requires the sharing of URLs for search results, including advanced search results. In the second place, the Commission considers this risk of copying to be low due to the limited number of advanced search URLs for each query. For example, a query "*hotels in brussels*" shows four URLs in the "*Places*" module and three URLs in the "*Hotels*" module, including only a single URL for each intermediator, such as [market participant] or [market participant].[498] By contrast, Alphabet's and third parties' inventories likely include hundreds or thousands of products (e.g., [market participant] lists approx.

---

492 [Market participant's] response to RFI PO 1 of 28 January 2026, page 8, Doc ID [...].

493 [Market participant's] submission dated 5 March 2024, page 2, Doc ID [...]. See also [market participant's] response to RFI 2 of 18 November 2025, Question 3, page 7, Doc ID [...]; [market participant's] reply to RFI 1 of 18 November 2025, Tranche 1, Question 2, page 4, Doc ID [...].

494 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], questions 8, 10 and 12; Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 16; Alphabet's reply to RFI 2 of 22 December 2023, Doc ID [...], question 7; Alphabet's reply to RFI 8 of 22 July 2025, Doc ID [...], questions 5 and 9.

495 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 10. This also addresses the concerns expressed in the public consultation responses, see the submission by [third party], [third party], Doc ID [...], [third party], Doc ID [...].

496 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 396, 403 and 480.

497 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 396, 403 and 480.

498 See the query "*hotels in Brussels*" *Google*, hotels in brussels - Google Search, Doc ID [...], last accessed 10 June 2026.

1000 hotels in Brussels).[499] As a result, the disclosure of a limited number of URLs is unlikely to provide meaningful information on third parties' product inventories and broader business strategy.

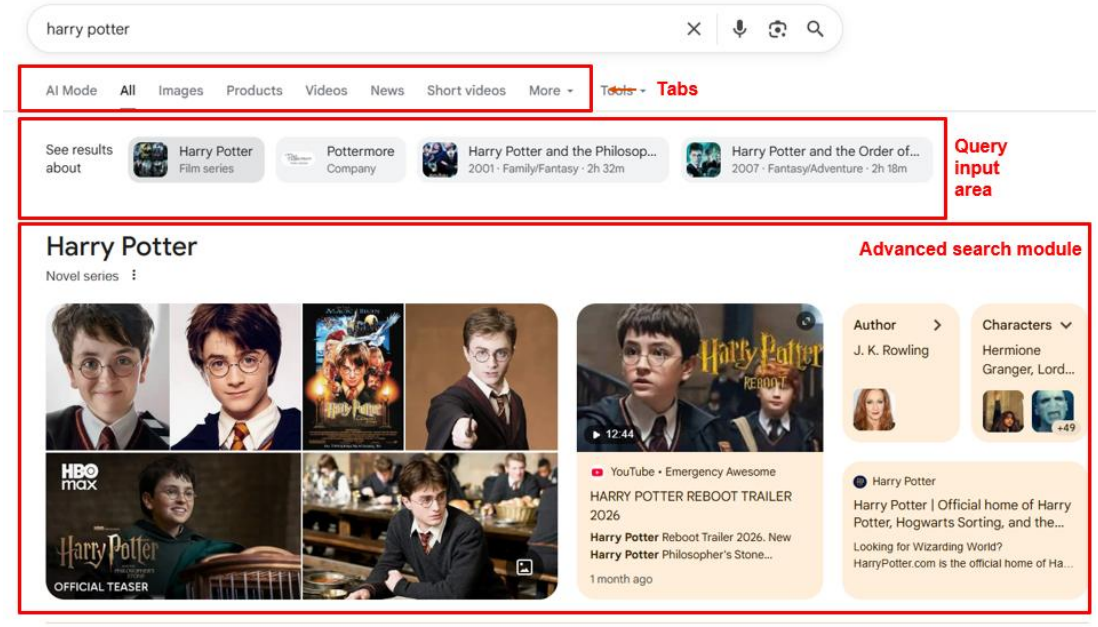
(348) **Seventh**, the Commission does not consider that the sharing of mere URLs displayed to users will create appreciable risks to Alphabet's trade secrets.[500] The identity of Alphabet's suppliers of advanced search results cannot be considered a trade secret or commercially sensitive information as their identity is displayed publicly as URLs on SERPs. Article 2(1)(b) of Directive (EU) 2016/943 provides that a trade secret exists only where *"it is not […] generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question."* As a matter of principle, information that has been put in the public domain for legitimate reasons – and therefore has become readily accessible, cannot be considered commercially sensitive.[501]

4.3.2.2.5. Description of visual elements

4.3.2.2.5.1. Introduction

(349) OSE's SERPs regularly include various visual elements beyond the plain-text components. Common visual SERP elements include tabs, query input areas, dedicated space on SERP for advanced and paid search modules, rich search results (with pictures, star ratings), image packs, videos, interactive widgets, etc. (see Figure 10).

Figure 10 – Visual elements on Google Search's SERP



Source: Own illustration

499 Specifically 1,033 properties are found for Brussels on 26 May 2026 for a single room for 2 adults without specifying check-in and check-out dates. See a query "*hotels in Brussels*" *[market participant's website]* , Doc ID [...], last accessed 10 June 2026.

500 Alphabet's reply to RFI 1 of 23 November 2023, Tranche 1, Doc ID [...], question 10.

501 See for example judgment of 5 October 2020, Casino, Guichard-Perrachon and AMC v Commission, T-249/17, EU:T:2020:458, paragraphs 263-267 and judgment of 30 September 2003, Atlantic Container Line and Others v Commission, T-191/98, T-212/98 to T-214/98, EU:T:2003:245, paragraph 1 154, See also OJ C 259, 21.7.2023, page 1–125, paragraph 338.

(350) The intersection between text SERP components and visual SERP components is blended. For example, currently OSEs no longer separate text search results from visual search results but rather integrate them into a unified search experience. While in the past a classic SERP consisted of search result titles and text snippets, today OSEs enhance such results with a range of visual elements, such as those described in the recital above.

(351) The Google Search Data does not include an individual category of data for visual elements. However, it includes certain visual elements which fall within the query and view data. In particular, the Google Search Data includes the query data in relation to the autocorrect function, query shortcut chips, autocomplete function, query suggestions, entity results, "*see results about*" feature and advanced search filters.[502] The Google Search Data also includes the view data in relation to tabs displayed on SERPs and the indication that SERPs include paid and advanced search modules.[503]

(352) The Commission's preliminary measures did not refer to the data on visual elements as distinct categories of data, however, they referred to them in relation to query and view data. This raised questions from Alphabet[504] on the actual scope of mandated data sharing in relation to visual elements and their content. This Decision specifies this in more detail.

4.3.2.2.5.2. The Commission's assessment

(353) As set out in section 4.3.2.2.1.2, the Commission specifies that Alphabet must share the (i) fact of displaying and the text included in query input areas, in query shortcut chips, entity results, query suggestions, "*see results about*" feature and similar, which are displayed on SERPs, (ii) the fact of displaying tabs on SERPs and their type, and (iii) the fact of displaying paid search modules and advanced search modules and their types, irrespective of whether such elements are displayed with or without an URL.

(354) With this measure the Commission specifies further the references to "*visual elements*" in the recitals specifying query, view, click and ranking data (see section 4.3.2.2.1.2). The Commission specifies that some elements on SERP which constitute view data can be visual in nature and the fact that they do not come with an URL is not an obstacle to data disclosure.[505]

(355) **First**, Alphabet is requested to share the fact of displaying and the text included in query input areas. In practice, this means sharing an information that a given query triggers query shortcut chips, query suggestions and other query input areas listed in recital (211)(a)(2) (e.g., the query "*Harry Potter*" triggers the "*See results about*" feature). This also means sharing the text displayed to user in query input areas (e.g., the "*See results about*" for "*Harry Potter*" includes "*Harry Potter – Film series*", "*harry Potter and the Philosophical Stone – 2001 – Family/Fantasy – 2h 32 m*" and "*Pottermore – Company*") (see the second box in Figure 10). The Commission considers this data is the view data. Query input areas are part of SERP and therefore constitute view data. In particular, Google Search shows them to users in response to their queries.

---

502 See recital (206).

503 See recital (275).

504 Alphabet's email dated 16 April 2026, Doc ID [...].

505 If a user clicks in a query input area and generates the query, this data is part of query data, as explained in recital (242).

(356) **Second**, Alphabet is requested to share the fact of displaying tabs on SERPs and their type. In practice, this means sharing the list of tabs which was displayed to user in response to their query (e.g., a query "*Harry Potter*" triggers the following tabs: AI Mode, All, Images, Products, Vidos, News, Short videos, Forums, Books, Web). As discussed in recital (279)(a)(4), the Commission considers URLs displayed to users as view data and requires Alphabet to share an identifier that a given URL was displayed as part of a specific tab. For clarity, Alphabet should also provide Search Data recipients with an information on the fact that a query led to a display of specific tabs as visual elements of SERPs, regardless of whether the user clicked or not on any specific tab (e.g., in the case of query "*Harry Potter*", the Search Data should include the list of tabs returned to the user (AI Mode, All, Images, etc), see the first box in Figure 10).

(357) **Third**, Alphabet is requested to share the fact of displaying paid search modules and advanced search modules and their types. In practice, this means the sharing of an information that a module of a given type was displayed in response to a query (e.g., the query "*Harry Potter*" triggers Entity results, Book carousel and About module, see third box in Figure 10). As discussed in sections 4.3.2.2.3 and 4.3.2.2.4 the Commission considers paid search modules and advanced search modules as view data. It consequently requests Alphabet to share advanced search URLs or a placeholder for paid search URLs, together with an identifier that they are included in advanced search and paid search modules, respectively, and their types. For clarity, Alphabet must also share the very information of displaying advanced search and paid search modules regardless of whether a search module at hand includes or not an URL. For example, for the query "*j. k. rowling age*", Google Search provides a direct answer "*60 years (July 31, 1965)*". In this case, the Search Data, should include the information that this query triggered an advanced search module and classify this module as a direct answer.

(358) **Fourth**, the Commission clarifies that this measure does not require Alphabet to share the visual "*content"*. As described in the recitals above, Alphabet should provide only the "*description"* of SERP *visual element* to enable third parties to understand the lay-out of SERP rather than share the actual visual content displayed on SERP, such as actual images, videos, interactive widgets, direct answers, rich content (e.g., star ratings) or the content of advanced search or paid search modules (e.g., for the query "*j. k. rowling age*", it is important to share the clickable text which can act as query input, but there is no need to share any further module content, such as a reference to the fact that J.K. Rowling is "*60 years (July 31, 1965)*"). This clarification addresses Alphabet's concern that the measures which require Alphabet to share the content of "*entity results*" and "*see results about*" features would disclose the content of its search advance modules.[506]

(359) **Fifth,** the Commission does not agree with Alphabet's view that the measures on visual elements duplicate the measures on query data, and in any event are not admissible as not covered in the Preliminary Findings.[507] In the first place, these measures go beyond the measures on query data.[508] They require Alphabet to share the data on the visual SERP components, including query modifiers (i.e., query modifiers *displayed* to the user rather than only those which were *clicked on*) and the SERP elements, which do not come with an URL (i.e., the fact of displaying tabs and advanced search modules regardless whether they include an URL). In the second

506 Alphabet's response to the Revised Measures, Doc ID […], paragraphs 66-67.

507 Alphabet's response to the Revised Measures, Doc ID […], paragraphs 63-69.

508 Contrary, Alphabet's response to the Revised Measures, Doc ID […], paragraph 64 and 68.

place, these measures were referred to in the Preliminary Findings, contrary to Alphabet's allegations.[509] In the section "*view data*", the preliminary measures required Alphabet to share the data on "*visual content which are displayed on search engine results pages*".[510] It is following Alphabet's request that the Commission clarifies this reference in more detail.[511] Alphabet also had several opportunities to exercise its rights of defence in relation to these measures. The Commission and Alphabet exchanged views on the visual elements in the meetings on 6 May 2026 and 10 June 2026. The exchanges on visual elements also took place in writing: the Commission sent to Alphabet the updated draft of the measures (including the measures on visual elements)[512] on 8 June 2026 and Alphabet submitted a response to the updated measures (including on visual elements) on 15 July 2026.[513]

4.3.2.3. Click data

(360) This section presents the measures related to click data and the underlying Commission's assessment. Section 4.3.2.3.1.1 provides a general introduction of click data; section 4.3.2.3.1.2 sets out the measures the Commission is specifying in relation to click data; section 4.3.2.3.1.3 provides the summary of gatekeeper's view, section 4.3.2.3.1.4 provides the Commissions' assessment underpinning the measures specified, and sections 4.3.2.3.2 to 4.3.2.3.4 provide further assessment in relation to specific types of click data covered by the measures.

4.3.2.3.1. General

4.3.2.3.1.1. Introduction

(361) Once presented with the results for their query, users interact with the search results in various ways, such as reviewing the results on the SERP, clicking on URLs, reviewing the pages the URLs lead to, coming back to the SERP and clicking on other URLs, modifying the query by clicking on a modification tool or entering a new query,[514] and abandoning the search altogether. Data on the user's interaction with the search results provides valuable information on the relevance of each of these results to the query entered by the user and is used for OSE services optimisation.

(362) The Google Search Data includes data on the number of clicks on the results contained in the dataset. For organic results, the click count is provided for the main blue link and any associated site links, taken together, and for advanced free search results and paid search results, the click count is aggregated per result type, i.e. the aggregate number of clicks on the advanced search block, and the aggregate number of clicks on paid results block.[515]

(363) For the reasons listed in sections 4.3.2.3.1.4, 4.3.2.3.2.2, 4.3.2.3.3.2, and 4.3.2.3.4.2, the Commission has decided specifying the measures listed in section 4.3.2.3.1.2.

---

509 Contrary, Alphabet's response to the Revised Measures, Doc ID […], paragraph 65.

510 Preliminary Findings, Annex, paragraph 6.

511 Alphabet's email dated 16 April 2026, Doc ID […].

512 Commission's email dated 8 June 2026, Doc ID […].

513 Alphabet's response to the Revised Measures, Doc ID […].

514 Query modification is discussed in Section 4.3.2.1.2 above and will not be further discussed in this section.

515 Alphabet's compliance report 2024, paragraph 107; Compliance report 2025, paragraph 97. Google's 6(11) DMA: Update on Progress with our Compliance Solution dated 19 April 2023.

4.3.2.3.1.2. Measures

(364) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, subject to anonymisation requirements, Alphabet must share with eligible third-party OSEs any data on user interaction with the SERP as displayed on the user's device, with any visual elements, and any URLs and with the pages linked by these URLs, including the type, order and duration (where relevant) of user actions, or lack thereof, on par with the data collected by Alphabet for the purpose of optimising its OSE services.

(365) It follows that Alphabet must share with eligible third-party OSEs at least the following click data for each URL or visual elements shared pursuant to the paragraphs concerning view data of these measures (together: "**SERP Element**"):

(a) Order and duration, or the absence of, clicks and clicks back (i.e. clicks indicating the user's return to the SERP following an earlier click) on the SERP Element;

(b) The duration a user viewed the given SERP Element;

(c) The duration, or the absence of, hovering on the SERP Element;

(d) The number, or the absence of, scrolls on the SERP;

(e) The occurrence, or the absence of, swipes within a swipeable SERP Element; and

(f) The occurrence, or the absence of, expansions of a SERP Element.

4.3.2.3.1.3. The gatekeeper's view

(366) Beyond its general claims that the measures expropriate its intellectual property and innovation, which are discussed in section 4.3.1 above, in relation to click data, Alphabet submits that the term "click data" in Article 6(11) of Regulation (EU) 2022/1925 means only "*data on the number of click a search result receives*", and should not be interpreted to extend to user interaction data as this interpretation is not supported by the legislation, nor by common understanding of the term click data and cannot be justified by views of foreign authorities or Alphabet's internal documents.[516] Alphabet further submits that any interpretation of the term "*click data*" requiring disclosure of data beyond "*the metrics that measure the number of clicks that results receive*" is unfounded.[517] Finally, Alphabet submits that it does not collect as a distinct data field or does not use some of the data types required to be shared under the measures concerning click data.[518]

4.3.2.3.1.4. The Commission's assessment

(367) The Commission considers that to meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, subject to anonymisation requirements, Alphabet must share with eligible third-party OSEs any data on user interaction with the SERP as displayed on the user's device, with any visual elements, and any URLs and with the pages linked by these URLs, including the type, order and duration (where relevant) of user actions, or lack thereof, on par with the data collected by Alphabet for the purpose of optimising its OSE services, for the following reasons.

---

516 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 436-453.

517 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 454-457.

518 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 486-487, Alphabet's response to the Revised Measures, Doc ID […]2, paragraph 61.

(368) **First**, the Commission considers that the term "*click data*" in Article 6(11) of Regulation (EU) 2022/1925 should be interpreted as referring to user interaction data, rather than applying only to user interaction through clicks.

(369) ***In the first place***, recital 61 of Regulation (EU) 2022/1925 demonstrates that the legislator's intention in relation to the term "*click data*" was to cover user interaction with the results presented to the user. The recital refers to ranking, query, click and view data collected by undertakings providing online search engines as "*information about what users searched for,* ***and how they interacted with, the results with which they were provided***" [emphasis added] and proceeds to clarify that the gatekeepers access to "***such*** […] ***data*****"**, i.e., also to data concerning user interaction with the SERP, constitutes a barriers to entry and expansions and that therefore the gatekeeper should provide access to "***those*** […] ***data*****",** i.e., also to data concerning user interaction with the SERP: "*Undertakings providing online search engines collect and store aggregated datasets containing* ***information about what users searched for, and how they interacted with, the results with which they were provided****. Undertakings providing online search engines collect* ***these data*** *from searches undertaken on their own online search engine and, where applicable, searches undertaken on the platforms of their downstream commercial partners. Access by gatekeepers to* ***such ranking, query, click and view data*** *constitutes an important barrier to entry and expansion, which undermines the contestability of online search engines. Gatekeepers should therefore be required to provide access, on fair, reasonable and non-discriminatory terms, to* ***those ranking, query, click and view data*** *in relation to free and paid search generated by consumers on online search engines to other undertakings providing such services, so that those third-party undertakings can optimise their services and contest the relevant core platform services*." [emphasis added]. Contrary to Alphabet's claim,[519] recital 61 does not simply observes, as a factual matter, that search engines collect user interaction data. The recital rather expresses a normative view specifically in relation to the user interaction data collected by undertakings providing online search engines. This view is therefore relevant for the interpretation of the term "*click data*" in Article 6(11) of the Regulation.

(370) ***In the second place***, the term "*click data*" commonly refers to data on user interaction with the SERP, in particular in the context of identifying user data which is used by OSEs. References to "*click data*", or "*click and query data*" as applying to user interaction generally can be found in reports by competition authorities and court decisions.[520] For example, in its 2024 report revisiting general search services, the Australian Competition and Consumer Commission stated that "*Click-and-query data includes data on the queries that users enter into a search engine, along with the actions they take in response to the results*";[521] the UK Competition and Markets Authority, in its online platforms and digital advertising market study referred to

519 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 437.

520 In relation to Alphabet's arguments against the references to views of foreign authorities (Alphabet's reply to the Preliminary Findings, paragraphs 443-444), the Commission notes that EU courts regularly refer to views expressed by foreign courts and competition authorities for relevant context. Views of the CMA, ACCC and the U.S court are brought to demonstrate that in the context of mapping user data used by OSEs, the term "click data" is commonly understood to cover user interaction more generally. Eventual differences in data disclosure obligations, which may be the result of different legal regimes, do not detract from the use of term "click data" to cover user interaction.

521 ACCC, Digital Platform Services Inquiry – September 2024 report revisiting general search services, issues paper published on 18 March 2024, pages 9 and 19, available at: https://www.accc.gov.au/system/files/dpsi-september-2024-report-issues-paper.pdf?ref=0&download=y (last accessed on 13 April 2026) (Doc ID […]).

click-and-query datasets as "*containing information about what consumers searched for and how they interacted with the results that they were served*". The study further explains that "*Useful interaction data may include, for example, dwell time on the search results page, whether the consumer scrolled down the page, whether the mouse hovered over a particular element, what links the consumer clicked and whether they hit the back button after following a link*".[522] Similarly, in its memorandum opinion of 5 August 2024, the United States District Court states that click data, "*includes the search results on which a user clicks; whether the user returns to the SERP and how quickly; how long a user hovers over SERP results; and the user's scrolling patterns on the SERP*".[523] The court further refers to user-interaction data and "*click-and-query*" data interchangeably,[524] and in particular to the data used by Google's ranking algorithms, Navboost and [Alphabet's internal system component], as "*click-and-query data"*.[525] [Description of Alphabet's internal system processes]. Several market participants support the view that the term "*click data*" should be interpreted to cover user interaction data.[526] The Commission notes that while some market participants do not consider the term "*click data*" to refer to user interaction data which is not measured by clicks, they note the importance of such data for OSE optimisation[527] and consider that such user interaction data falls under other data categories mentioned in Article 6(11) of the regulation, namely "*view data*".[528] Alphabet's submissions[529] that the definition of "*click*" in computing and in computer science literature on search evolution does not extend beyond explicit clicks is irrelevant. The term "*click data*" is broader than "*click*", and anyway, as demonstrated above, the term "click data" has been used repeatedly to cover user data which goes beyond mere clicks.

(371) ***In the third place***, Alphabet itself uses the terms clicks and user interaction interchangeably, thus further demonstrating that the OSE industry sees the term "*click data*" as referring to user interaction. This is evident from Alphabet's internal documents, as well as statements made by Alphabet's employees. For example, an internal Google presentation titled "*Life of Click (user-interaction)*" states that "*we may use "clicks" as a stand-in for "user-interactions" in some places. User-interactions include clicks, attention on a result, swipes on carousels and entering a*

---

522 CMA, Online Platforms and Digital Advertising market study, Appendix I: search quality and economies of scale (2020) [online], paragraphs 29-30, Available at: https://assets.publishing.service.gov.uk/media/5fe4957c8fa8f56aeff87c12/Appendix_I_-_search_quality_v.3_WEB_.pdf (last accessed on 13 April 2026) (Doc ID […]).

523 United States of America v. Google LLC, Case No. 20-cv-3010 (APM) Document 1033, paragraph 88 , Doc ID 1966. See also the court's memorandum opinion dated 2 September 2025, where the court refers to user interaction data as click and query data, stating that "Examples of such data include the web link or vertical information the user clicks on, how long a user hovers over a link, and whether the user clicks back from a web page and how quickly." United States of America v. Google LLC, Case 1:20-cv-03010-APM Document 1436, page 152, Doc ID […].

524 US V. Google, memorandum opinion dated 2 September 2025, page 152 (Case 1:20-cv-03010-APM, Document 1436), Doc ID […].

525 US V. Google, memorandum opinion dated 2 September 2025, page 153 (Case 1:20-cv-03010-APM Document 1436), Doc ID […].

526 See: replies to RFI 1 of 28 January 2026 of: [market participant] Doc ID 1883-4, question 3; [market participant], Doc ID […], question 3, [market participant], Doc ID […], question 4, and [market participant] Doc ID […], question 7. Reply of a market participant to RFI 1 of 17 February 2026, Doc ID […], question 9.

527 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 3.

528 See: replies to RFI 1 of 28 January 2026 of [market participant] Doc ID […], question 8 and [market participant] Doc ID […], question 6.

529 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 439.

new query".[530] Another internal document [direct quote describing Alphabet's internal definition of data type].[531] [Direct quotes describing Alphabet's internal system components and definition of data types].[532] [Description of Alphabet's internal processes][533] [descritption of Alphabet's internal definition of data type].

(372) ***In the fourth place***, a narrow interpretation limiting "*click data*" only to the number of clicks generated per result would exclude a significant amount of data which is important for OSE optimisation, in particular in the mobile search era in which clicks are replaced by interactions indicating the user's attention, such as dwell time and swipes serve to demonstrate user satisfaction. With the increase of mobile search, excluding such a large share of search data therefore goes against the objectives of Article 6(11) and of Regulation (EU) 2022/1925. This further supports the understanding that the Regulation was not intended to exclude user interaction data which is not strictly measured by clicks.

(373) In this respect, Google's internal documents demonstrate [description of Alphabet's internal documents].[534] One of these documents[535] [direct quotes describing Alphabet's internal interpretation of data][536] [Description of Alphabet's internal interpretation of data].[537] Another Google internal document further [direct quotes describing Alphabet's internal interpretation of data].[538] [Description of Alphabet's internal measurement of user interaction]:[539]

Figure 11: Alphabet's internal document titled [Alphabet's internal system component]

[Image displaying Alphabet's internal measurement of user interaction]

Source: Alphabet's reply to RFI 10, Annex 14.5, slide 22.

(374) The Commission notes that, contrary to Alphabet's claims,[540] the fact that Alphabet is not required to share the content of modules such as direct answers with eligible third party OSEs, does not mean that data on user interaction with such modules has no utility for the third parties. Even in the absence the content of such modules, user interaction with them provides valuable information on user intent. For example, attention to advanced results module can inform the OSE that the user query was not navigational. In addition, as explained in recital (383) of this Decision, to understand users' intent, OSEs require user interaction data for everything displayed on the SERP.

(375) The importance for OSE optimisation, of user interaction data which is not strictly measured by clicks is also confirmed by third parties. One market participant explained that such data would assist "[a]ddressing the "*Zero-Click" Problem. In*

530 Alphabet's reply to RFI10 of 12 November 2025, Annex 14.9, page 3, Doc ID […].

531 [Description of Alphabet's internal processes in relation to data type]. See Alphabet's reply to RFI 12 of 13 November 2025, Doc ID […], Annex Q1.6, page 2.

532 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.11, Doc ID […].

533 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 445-450.

534 [Description of Alphabet's internal system processes and components] (see: Alphabet's reply to question 11 of RFI 2 dated 30 January 2026, Doc ID […]).

535 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.3: Ranking newsletter dated 7 March 2016, Doc ID […].

536 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.3: Ranking newsletter dated 7 March 2016, page 2, Doc ID […].

537 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.3: Ranking newsletter dated 7 March 2016, page 3, Doc ID […]6.

538 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.5, slide 19, Doc ID […].

539 See also Alphabet's reply to RFI10 Annex 14.7, slide 4, Doc ID […], [Description of Alphabet's internal measurement of user interaction].

540 Alphabet's response to the Revised Measures, Doc ID […], paragraph 59.

modern search many users find their answer directly in a generated summary or search snippet without clicking any source link. […] *User engagement with these AI-generated responses—demonstrated through hover time, deliberate scrolling, and low abandonment rates—validates the relevance and authority of the cited URLs, providing meaningful training signals even absent direct clicks*".[541] Another market participant explained that "*non-click interaction data* […] *may be used* […] *to assess result usefulness and user experience – for example, as indications of engagement, possible dissatisfaction, or query reformulation".*[542]

(376) Excluding such data solely on the basis that it is not strictly measured by clicks would maintain the data asymmetry between competing OSEs and the gatekeeper, who would continue enjoying the scale advantage in relation to a large share of user interaction data, constituting an important barrier to third party OSEs' entry and expansion. [Description of Alphabet's measurement of user interaction], as explained by Alphabet's internal document,[543] further support the conclusion that it could have not been the legislator's intention to cover desktop focused user data. An interpretation of "*click data*" as applying to user interaction would allow an effective, future proof implementation of Regulation (EU) 2022/1925 based on its objectives and should therefore be preferred.

(377) ***In the fifth place***, even if "*click data*" is interpreted more narrowly than user interaction data, *quod non*, the data shared by Alphabet should be broader than click count per result. The term "*click data*" is broader than the term "*clicks*". If the legislature had intended to limit the scope of Article 6(11) of Regulation (EU) 2022/1925 to the number of clicks, it would have used the term "*clicks*". Instead, it chose the term "*click data*" which is a broader category.

(378) At a minimum, the following "*click data*" should be included under Article 6(11) of Regulation (EU) 2022/1925:[544] [545]

(a) **Data which is related to clicks**, i.e., data on the order and duration, or the absence of clicks and clicks back (see recital (365)(a) of this Decision). As explained in Section 4.3.2.3.2, all these data types are strictly related to clicks and constitute core aspects of click data. As such they constitute "*click data*";[546]

(b) **Data which is measured through clicks**, i.e., the duration a user viewed a given search result (see recital (365)(b) of this Decision) and the occurrence or the absence of expansions of a search result (see recital (365)(f) of this Decision). As explained in sections 4.3.2.3.3 and 4.3.2.3.4 of this Decision, these data types are measured through or recorded as click events, and are both required for OSE optimisation. Expansions are tracked as click events on the expansion feature and the duration a user viewed a given search result is

---

541 A market participant's reply to RFI of 17 February 2026, Doc ID […], question 9.

542 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 3.

543 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.3: Ranking newsletter dated 7 March 2016, Doc ID […].

544 Under this interpretation, data concerning the duration or absence of hovering on a given search result does not constitute click data.

545 Contrary to Alphabet's claim in its Response to the Revised Measures (Doc ID […] paragraph 58), and as demonstrated below all three data groups below are closely related to clicks, either because they provide further information on clicks, or because they are measured through clicks, or because they resemble clicks in a mouse free environment.

546 In addition to qualifying as data which is related to clicks, these data types are also measured through clicks.

measured by the time that passed from the moment the search results were presented to the user until the moment the user clicked on one of the results. As such, they constitute "*click data*";

(c) **Data on actions which resemble clicks on mobile devices**, i.e., the number or absence of scrolls on the SERP and the occurrence or the absence of swipes withing a swipeable SERP Element (see recitals (365)(d) and (365)(e) of this Decision). As explained in section 4.3.2.3.4, at least on mobile devices, which do not require the use of a mouse, there is not much difference between the actions of scrolling and swiping and the action of clicking on a result, as they are all performed through touching and taping the device's screen. As such they constitute "*click data*".

(379) **Second**, for the reasons listed in section 4.3.1.3, subject to anonymisation requirements, Alphabet must share any user interaction data which it collects for the purpose of optimising its OSE services.

(380) **Third,** user interaction data should be shared for all search results, regardless of their type.

(381) ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 requires the provision of ranking, query, click and view data "*in relation to free and paid search*". Article 2(23) of the Regulation further clarifies that search results cover "*any information in any format* […] *irrespective of whether the information returned is a paid or an unpaid result, a direct answer or any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them*".

(382) ***In the second place***, Alphabet confirmed that it collects user interaction data for all types of search results, including organic, advanced and paid search results.[547] The principle of parity therefore requires Alphabet to share this data with third party beneficiaries. As explained in section 4.3.1.3, the Commission considers that the display of paid search results on the SERPs constitutes part of OSE services. Therefore, the fact that Alphabet collects and uses user data related to paid search results for optimising the presentation of search ads on the SERPs amounts to Alphabet collecting this data for the purpose of optimising its OSE services and it is sufficient for the inclusion of this data in compliance with the parity principle. [Description of Alphabet's use of data]. As explained in section 4.3.2.2.3, paid search results constitute a substantial part of the SERP. The definition of "*search results*" in Article 2, point (23), of Regulation (EU) 2022/1925 confirms that paid search results returned in response to a user query form part of the online search engine services. [Description of Alphabet's use of data].

(383) ***In the third place***, to understand users' intent, OSEs require user interaction data for everything displayed on the SERP. In particular, relying on user interaction data only for organic results provides an incomplete and distorted picture. Alphabet's internal documents [direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction][548] The document further states that [direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction].[549] Another document clearly states that [direct quotes describing Alphabet's internal system processes and components, and

547 Alphabet's reply to questions 31 and 32 of RFI 2 of 30 January 2026, Doc ID […].
548 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 3.
549 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 4.

measurement of user interaction].[550] The documents explain that [direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction].[551] According to this internal document, [direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction].[552]

(384) In this respect, market participants noted that "*Understanding what a user clicks on in response to a query, whether it be a static link or a dynamic answer block, is critical to machine learning to understand user intent – which in turn feeds directly into improving relevance and ranking*";[553] "*advanced units above organic results* […] *strongly influence click behaviour"*;[554] "[…] *click data should include not only clicks from the organic URLs, but also clicks on ad URLs and URLs in modules. We need to be able to distinguish between the kinds of URLs being clicked (i.e. know whether a clicked URL was organic, in a module, or in an ad)*".[555] One market participant referred to the importance of understanding which response modules are the most clicked on to OSE's competitiveness.[556]

(385) **Fourth,** the data should be provided in a non-aggregated manner. ***In the first place***, there is nothing in Regulation (EU) 2022/1925 to suggest that the click data for non-organic results and for links and sub-links should be provided in an aggregated manner and not individually. ***In the second place,*** […] the principle of parity requires Alphabet to share the data at the same level of granularity. [Direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction].[557] [Direct quotes describing Alphabet's internal system processes and components, and measurement of user interaction].[558] ***In the third place***, aggregating click data for non-organic results excludes important information on the relevance of various non-organic search results to the user's query, thus not allowing third party OSEs to "*optimise their services and contest the relevant core platform services*". This is important in particular in relation to advanced search results, where the individual results may differ from each other, and where aggregating click data would conceal such differences. In this respect, one market participant noted that "[e]*ffective optimisation requires granular, per-result click data that is directly tied to individual queries, result positions, and UI contexts […] aggregate click counts* […] *do not allow* […] *to distinguish between different types of user engagement or to reliably infer user satisfaction*".[559] Another market participant explained that "[w]*hen click data is aggregated, it misses crucial signals, such as: 1. The position/rank of the URL when it was clicked* […] *2. The order and timing of URL clicks (and bounce-backs)* […] 3. *Which URLs were presented to the user above/around the clicked URL*".[560] ***In the fourth place***, given that due to the anonymisation requirements, no URLs will be provided for paid search results (see section 4.4.4.1), the Commission considers that sharing user interaction data for

550 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.5, Doc ID […], page 3.
551 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 1.
552 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 2.
553 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question.
554 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.
555 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 2.
556 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 9.
557 Alphabet's reply to question 14 of EC RFI 2 dated 30 January 2026, Doc ID […].
558 Alphabet's reply to question 32 of EC RFI 2 dated 30 January 2026, Doc ID […].
559 [Market participant]'s reply to RFI 1 of 18 November 2025 (tranche 2), Doc ID […], question 3.
560 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

anonymised paid search results, will not disclose sensitive commercial information of Alphabet and third-party advertisers.

(386) **Fifth,** applying the principle of parity requires the sharing of this data. As explained in more detail in sections 4.3.2.3.2, 4.3.2.3.3 and 4.3.2.3.4, Alphabet collects a wide range of user interaction data and uses it for its OSE optimisation. As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(387) **Sixth**, user interaction data is crucial for OSE optimisation. After delivering search results in response to a user query, OSEs rely on user interaction to interpret users' intent and relevance to their queries. The users' interaction is logged and used as feedback to the quality of the results presented on the SERP. User interaction is used to verify whether the results satisfied the user, which results were most relevant, which were not relevant at all. To ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, such data should be covered by the data obligation specified in Article 6(11) of Regulation (EU) 2022/1925.

(388) ***In the first place***, the importance of user interaction data is acknowledged by Alphabet, in reply to Commission's RFIs and in its internal documents. An internal Alphabet presentation explains that logging of and learning from user interaction is key for search to work well.[561] The document notes that "*as people interact with search, their actions teach us about the world. For example, a click might tell us that an image was better than a web result. Or a long look might mean a KP was interesting. We log these actions, and then scoring terms extract both narrow and general patterns.* […] *The source of Google's magic is this two-way dialogue with users. With every query, we give some knowledge, and get a little back.*"[562] The document further explains how the SERP serves to implicitly ask users about the quality of the search results. For example, in relation to a SERP with 10 blue links: "*[T]he ten blue links implicitly pose the question, 'Which result is best?" Result previews give background. And the answer is a click.*"[563] [Description of Alphabet's internal system processes].[564]

(389) ***In the second place***, third parties further emphasise the importance of user interaction for OSE optimisation. Market participants explain that "[c]*lick data is a strong signal that a URL is relevant to a query"*;[565] that user interaction data would allow them to develop more accurate ranking models and train specific ranking signals for each market,[566] and that (among other data) click data enables optimisation for "*what users actually find relevant inside the entire Ranking*

---

561 Document submitted as trial exhibit UPX0228 in U.S vs. Google case 1:20-cv-03010-APM, Doc ID […].

562 Document submitted as trial exhibit UPX0228 in U.S vs. Google case 1:20-cv-03010-APM, Doc ID […].

563 Document submitted as trial exhibit UPX0228 in U.S vs. Google case 1:20-cv-03010-APM, Doc ID […].

564 Alphabet's reply to RFI 8 of 22 July 2024, questions 10, 11, Doc ID […].

565 [Market participant]'s reply to RFI 1 of 18 November 2025. Doc ID […], question 3.

566 [Market participant]'s reply to RFI of 18 November 2025, Doc ID […], question 1;

page".[567] One market participant explained that access to behavioural data concerning user clicks (including, for example, long clicks, good clicks and exploratory clicks), views (such as expansion of menus or viewport features), time spent (on the result pages and on third-party sites), scrolls (up/down and horizontal actions), and actions on the web page (such as where users click on the webpage after leaving the results page) generally allows OSEs to optimise their search results to align with what would most satisfy users.[568]

(390) **Seventh**, sharing this data would not allow copying of Alphabet's technologies, nor would it discourage innovation. The measures do not require the sharing of Alphabet's algorithms or signals, but rather data generated by users, that would allow third-party OSEs to develop signals of their own. In particular, the measures do not require Alphabet to share how it interprets each user action, how it encodes user actions to derive the user intent, the weight given to user actions to assess user's intent or the intent Alphabet derives from the actions. The measures only require Alphabet to share the raw data about the user actions. This data would not reveal, and therefore not allow the copying of Alphabet's algorithms. Moreover, according to Alphabet itself, its ranking algorithms are very complex, and rely on many signals, [description of Alphabet's internal systems] but rather on Alphabet's own efforts. [Direct quote describing Alphabet's internal system processes].[569]

(391) Sections 4.3.2.3.2 to 4.3.2.3.4 below further discuss specific elements included under click data.

4.3.2.3.2. Order and duration of clicks

4.3.2.3.2.1. Introduction

(392) Information about the duration and order of the clicks, as well as absence thereof, serves as feedback on the perceived relevance of the results to the user's query, and is therefore used for OSE optimisation.

(393) The Google Search Data does not include data on the order and duration of clicks.

4.3.2.3.2.2. The Commission's assessment

(394) As set out in section 4.3.2.3.1.2, recital (365)(a) of this Decision, the Commission considers that to meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must share with eligible third-party OSEs, for each SERP Element, the order and duration, or the absence of, clicks and clicks back (i.e., clicks indicating the user's return to the SERP following an earlier click) on the SERP Element. [570]

(395) Below, the Commission provides reasons, additional to those provided in section 4.3.2.3.1.4, as to why it is specifying this measure.

(396) **First**, the data forms part of click data under Article 6(11) Regulation (EU) 2022/1925. ***In the first place*****,** as explained in recitals (368) *et seq*., the term "*click data*" should be interpreted to apply to all user interaction data. ***In the second place*****,** data on the order and duration, or the absence of, clicks and clicks back, clearly falls under "*click data*". The term "*click data*" is broader than the term "*clicks*". If the legislature had intended to limit the scope of Article 6(11) of the Regulation to the

567 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question.

568 [Market participant]'s reply RFI 1 of 18 November 2025 (tranche 1), Doc ID […], question 2.

569 Alphabet's reply to RFI8 of 22 July 2024, question 10, Doc ID […].

570 The text of the measure is repeated here for ease of reading, the binding text is provided in the Annex to this Decision.

number of clicks, it would have used the term "*clicks*". Instead, it chose the term "*click data*" which is a broader category. The order and duration of clicks and clicks back, as well as their absence, are all core aspects of clicks. As explained in the subsequent recitals, all these aspects of click data are essential for OSE optimisation. ***In the third place*****,** data on the order and duration, or the absence of, clicks and clicks back are all measured through clicks (or the absence thereof) and as such constitutes click data.

(397) **Second**, applying the principle of parity requires the sharing of this data, which Alphabet itself collects and uses for the optimisation of its OSE. ***In the first place***, Alphabet collects a wide range of data related to clicks. [Description of Alphabet's measurement of user interaction].[571] [Description of Alphabet's internal system processes and components].[572] [Description of Alphabet's internal system processes and components],[573] [description of Alphabet's internal system processes][574], [description of Alphabet's internal system processes].[575] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties. ***In the second place***, [description of Alphabet's internal system processes and components][576] [description of Alphabet's internal system processes and components]. In any case, Alphabet may also share data that would allow eligible beneficiaries to infer the order of clicks and click backs, to the extent this would equally allow beneficiaries to have the same data listed in the measure. The Commission further notes that Alphabet's claim [direct quote describing Alphabet's internal system processes and components][577] appears fully contradictory to its statements in reply to the Commission's RFIs.[578]

(398) **Third**, the data is required for OSE optimisation. Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as indicated in recital 61, such data should be covered by the obligation of Article 6(11) of Regulation (EU) 2022/1925. The order and duration of clicks provide valuable information on users' satisfaction with the search results and serves as feedback on the results' relevance to the user's query. If a user clicks on a result

---

571 Alphabet's reply to RFI10 of 12 November 2025, Annex Q5, Doc ID […].

572 [Description of Alphabet's internal processes]. See Alphabet's reply to question 1(e) of EC RFI 8 dated 19 February 2026, Doc ID […].

573 Alphabet's reply to RFI10 of 12 November 2025, Annex Q1.2, Doc ID 781;[Description of Alphabet's internal system processes and components]. See Alphabet's reply to questions 15 and 29 of RFI 2 dated 30 January 2026, Doc ID […]. [Description of Alphabet's internal system processes]. See, Alphabet's reply to question 1(d) of EC RFI 8 dated 19 February 2026, Doc ID […].

574 [Description of Alphabet's internal system processes and components]. See: Alphabet's reply to question 15 of EC RFI 2 dated 30 January 2026, Doc ID […].

575 Alphabet's reply to RFI10 Follow-up, Annex Q1, Doc ID […]; Alphabet's reply to question 3 of EC RFI 8 dated 19 February 2026, Doc ID […].

576 [Description of Alphabet's internal system processes and components]. See: Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 487, Alphabet's response to the Revised Measures, Doc ID […], paragraph 61.

577 Alphabet's response to the Revised Measures, Doc ID […], paragraph 61.

578 In its reply to RFI 10 Follow-up of 7 January 2026, Annex Q1, Doc ID […], [description of Alphabet's internal system processes and components]. In reply to question 1(e) of RFI 8 of 19 February 2026, Doc ID […], [Description of Alphabet's measurements of user interaction].

and then quickly clicks back to the SERP and clicks on another result, the short duration between the user's clicks may indicate the irrelevance of the first result to the user's search. A long duration before the user returns to the SERP or the absence of additional subsequent clicks after the first one may indicate the strong relevance of the clicked result to the user's query. The absence of clicks altogether may indicate (in connection with other signs of user attention) that the information displayed on the SERP was sufficient to satisfy the user query, or, to the contrary, that the search results failed entirely to satisfy the user's intent. This is particularly relevant for advanced search results, such as direct answers.

(399) ***In the first place***, this is confirmed by Alphabet's internal documents and replies to RFIs. Alphabet's internal documents refer, for example to [direct quote describing Alphabet's measurement of user interaction].[579] Another document [direct quote describing Alphabet's internal system processes and components].[580] [Direct quote describing Alphabet's internal system processes and components].[581] [Direct quote describing Alphabet's internal system processes and components].[582]

(400) ***In the second place***, the necessity and importance of this data to OSE optimisation is further confirmed by third parties:

(401) Market participants consider data on *clicks* to be essential to OSE optimisation: the average rating by market participants who replied to the Commission's RFI for the importance of clicks to OSE optimisation, on a scale from 1 to 5, was 5 for clicks on *organic* search results, 4.7 for clicks on *advanced* search results, and 4.6 for clicks on *paid* search results.[583] Market participants explained that "*raw queries and associated clicks can help with index quality and inferring search intent*",[584] that "*Clicks* […] *are a core optimisation input*",[585] a *"strong signal that URL is relevant to query*",[586] and that "*clicks on organic links* […] *signal that a user is satisfied with a standard web result.*[587] Market participants further explained that advanced search results "*materially affect user behaviour*";[588] and that "*Module clicks indicate relevance of specialized content*".[589] As for clicks on paid search result, market participants explained that the data is "[v]*ery important for optimisation across paid search*";[590] that "*Ad clicks indicate relevance and user intent";*[591] and that "*data on paid search clicks is essential to contextualise and correct the data regarding organic performance. Without knowing which ads were present and clicked, organic click patterns appear "artificially distorted"*".[592]

---

579 Alphabet's reply to RFI10, Annex 14.9, page 23, Doc ID […].
580 Alphabet's reply to RFI 10, Annex 14.5, slides 21-22, Doc ID […].
581 Alphabet's reply to RFI 10, Annex 14.5, slide 22, Doc ID […].
582 Alphabet's reply to RFI 10, question 1(c), Doc ID […].
583 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1 (Doc ID […]).
584 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 4.
585 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].
586 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].
587 [Market participant]'s reply to RFI of 28 January 2026, Annex 1, Doc ID […].
588 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].
589 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].
590 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […]
591 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].
592 [Market participant]'s reply to RFI of 28 January 2026, Annex 1, Doc ID […].

(402) Market participants further consider data on click back and click back time[593] to be very important to OSE optimisation: the average rating by market participants who replied to the Commission's RFI for the importance of click back and click back time to OSE optimisation, on a scale from 1 to 5, was 4.4.[594] Market participants explained that "[c]*lick back data provides meaningful feedback about the quality of the search results displayed, which improves directly ranking algorithms and helps identify low-quality/spammy websites*";[595] "*optimisation requires access to click data that is broken down into meaningful behavioural categories, including* […] *"long clicks"*[596] *that indicate deeper engagement with a result* […] *these distinctions are usually critical for training and calibrating relevance, ranking, and answer-quality models. Different click types carry different informational value; for example, a long click on a lower-ranked result may indicate a ranking failure*";[597] One market participant referred to the order and timing of clicks and bounce-backs as crucial signals, and explained that "[i]*f a user clicks a result and then quickly bounces back to the SERP and quickly clicks another result, then that is a strong signal that the first URL was not relevant after all*".[598] Other market participants explained that "[i]*f a user returns to the search page in under 10 seconds (a "Short Click" or Pogo-sticking), the algorithm learns that the result was likely a mismatch for that query. Without this data, a search engine is "blind" to the quality of the pages it recommend*";[599] "*Quick bounce-backs indicate irrelevant results*" whereas "*Longer dwell time on destination site indicates relevance*";[600] that click-back data is "*Essential negative feedback. Returning to the SERP shortly after a click often indicates poor relevance/quality of the clicked result; critical for optimisation*";[601] and that click-back time is "[v]*ery important complement to click-back: distinguishes "bad clicks" (quick returns) from longer engagements, improving relevance feedback quality*",[602]

(403) In relation to *click duration*, market participants explained that "[a] *low TTFC* [time to first click, i.e., the delta between the search results loading and the user making a choice] *across many users suggests that the "Title" and "Snippet" (description) are*

---

593 While the question's text referred to click back *time*, as evident from the quotes provided below, the replies refer mainly to click back *duration, e.g.* through references to *long* and *short* click back time.

594 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1,Doc ID […].

595 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3. see also [market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 5, specifying that the information required for OSE optimisation includes, among others, the click event timestamp; an indicator and timestamp for the return/back event (or, more generally, evidence that the user resumed interaction with the results page or issued a subsequent query); the time elapsed between click and return (i.e., dwell time on the clicked result / time-to-return); where available, dwell time on the results page following the query (i.e., time spent on the SERP before any click or after returning); and where applicable, subsequent user actions such as an additional click on a different result for the same query, abandonment, or a reformulated/next query (including whether the original query was corrected or modified).

596 i.e., "*[c]licks where users spend a meaningful amount of time on a result without returning immediately to the search page*", see [market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 5.

597 [Market participant]'s reply to RFI 1 of 18 November 2025 (tranche 2), Doc ID […], question 3.

598 [Market participant]'s reply to RFI 1 of 18 November 2025 Doc ID […], question 3.

599 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 7.

600 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].

601 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].

602 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].

highly effective and the result is likely a match",[603] and that "*optimisation requires access to click data that is broken down into meaningful behavioural categories, including* […] *"good clicks" that indicate short-path satisfaction."*[604]

(404) The average rating by market participants who replied to the Commission's RFI for the importance of *click order/ click time stamp* to OSE optimisation was 3.4 on a scale from 1-5.[605] Market participants explained that the data "*Supports reconstruction of interaction flows (especially when combined with click-back and dwell time)*";[606] "*The order and timing of URL clicks (and bounce-backs)*[] *are crucial signals* […] *Timing patterns reveal relevance in ways aggregated data cannot capture*",[607] and that this data "*will be important to detect bot / spam behaviour, if included in the data set*".[608]

(405) Finally, in relation to the absence of clicks, market participants explained that "*the absence of clicks* […] *is equally important* [as clicks]*, for example, if a user instead focuses their click distribution on additional search features*".[609] Market participants explained that "no click impressions", i.e. "*instances in which a result (or a search engine results page) was displayed to a user but did not receive any click within the relevant session or attribution window* […] *constitute the key denominator for calculating* [click-through rate] *and for identifying patterns of abandonment. They enable the assessment of ranking quality even in situations where users do not click on any result, for example because the desired information was obtained directly from the results page*";[610] that "*If a user types a query, scrolls to the bottom, and then closes the tab without clicking, it's a massive signal that the search engine failed entirely for that specific intent*";[611] and that "*repeated scrolling or expansions without clicks may indicate unmet intent or inadequate presentation.*";[612] The average rating by market participants who replied to the Commission's RFI for the importance of abandonments data to OSE optimisation was 3.4 on a scale from 1-5.[613] One market participant noted that this is a "*Very important negative signal (no satisfactory engagement). Complements dwell-time-on-SERP and click-back signals to identify unsatisfied queries*".[614]

(406) **Fourth**, for the reasons listed in recitals (380) to (384) of this Decision, the data should be shared for all search results, regardless of their type.

(407) **Fifth**, for the reason listed in recital (385) of this Decision, the data should be provided in a non-aggregated manner.

---

603 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 7.

604 [Market participant]'s reply to RFI 1 of 18 November 2025 (tranche 2), Doc ID […], question 3.

605 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

606 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].

607 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […].

608 [Market participant]'s reply to RFI of 28 January 2026, Annex 1, Doc ID […].

609 [Market participant]'s reply to RFI of 28 January 2026, Annex 1, Doc ID […].

610 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 8.

611 [Market participant]'s reply to RFI 1 of 28 January 2026, Doc ID […], question 7.

612 [Market participant]'s reply to RFI 1 of 18 November 2025 (tranche 2), Doc ID […], question 3.

613 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

614 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 Doc ID […]

(408) **Sixth**, contrary to what Alphabet suggests, the fact that click back duration concerns the time a user spent on another website[615] is irrelevant to this assessment. The click back duration is measured through clicks on the SERP. This is what allows Google Search to collect and use the data, and therefore, the fact that during this time the user interacts with another page is irrelevant. In addition, Alphabet's statement that most of the metrics concerning data which related to clicks or measured through clicks "*are not in fact data about interactions with Google's results at all*" but rather about the "*user's interaction with the websites to which clicks on Google's results lead*",[616] is artificial, as the user interaction with these websites is a result of a query, it starts and ends through the SERP and is of outmost relevance for assessing the quality of the search results.

(409) **Seventh**, sharing this data would not allow copying of Alphabet's technologies, nor would it discourage innovation. Further to the reasons listed in recital (390), the measures do not require the sharing of the relevant time intervals that are used as indicators of good or inferior quality and relevance of the search results. Meaning, that the data would not allow beneficiaries to understand how Alphabet encodes and interprets click durations. In particular, Alphabet is only required to share the raw click duration. Alphabet is not required to specify what click duration, in its view, represents user's satisfaction and what click duration represents user dissatisfaction.

(410) **Eighth,** contrary to Alphabet's claim, a mere disclosure of URLs and clicks is unlikely to appropriate inventory information of third-party websites, by revealing, e.g., what products, hotel rooms, flights, or local businesses the websites in question have in their inventory, and how well a particular product is doing, and in any case the disclosure of clicks on paid search results was required by the legislator.[617] ***In the first place***, as explained in recitals (380) to (384), Article 6(11) of Regulation (EU)2022/1925 requires the sharing of click data for paid search results. ***In the second place***, the Commission considers the risk that clicks on advanced search URLs could reveal publishers' commercial and financial performance to be low.[618] This is because a product's (e.g., a hotel's) performance is determined by a complex array of factors, including actual reservations, revenues, cost structure, operating efficiency, and more. Moreover, clicks on Google Search represent only a fraction of end users' interest in a product, as demand can also come from a variety of other sources, including intermediation websites, the product's own website, travel agencies, corporate and contract sales, social media, loyalty systems, and more. Therefore, the risk of disclosing publishers' commercial and financial performance through the disclosure of clicks on advanced search URLs appears to be marginal at best.

4.3.2.3.3. Dwell time

4.3.2.3.3.1. Introduction

(411) Dwell time refers to the time a user spent reviewing the search results after entering a query. This data provides meaningful information on the user's satisfaction with the

---

615 See Alphabet's reply to RFI10, question 1(c): "*The duration it takes a user to come back to Google after a click on a result. This is not data about a user's interaction with a Google result at all. It is data about the user's interaction with the website to which a Google result referred the user – it measures how long that user spends on the website and stays away from Google*." See also Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 456.

616 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 456.

617 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 396, 403 and 480.

618 This claim was also made by several respondents to the Public Consultation, see for example, submissions of [association], Doc ID […]; [association], Doc ID […]; [association], Doc ID […].

results presented to it. The view time for a specific result is inferred from data about the user's viewport, i.e. the area of the webpage which is visible on the user's device, the elements of the SERP visible on the user's viewport and the time spent reviewing a specific viewport.

(412) The Google Search Data does not include any dwell time data.

4.3.2.3.3.2. The Commission's assessment

(413) As set out in section 4.3.2.3.1.2, recital (365)(b), the Commission considers that to meet the requirements of Article 6(11) of Regulation (EU) 2022/1925 Alphabet must share with eligible third-party OSEs for each SERP Element, the duration a user viewed the given SERP Element.[619]

(414) Below, the Commission provides reasons, additional to those provided in section 4.3.2.3.1.4, as to why it is specifying this measure.

(415) **First**, the data falls under Article 6(11) Regulation (EU) 2022/1925. ***In the first place*****,** as explained in recitals (368) *et seq.,* above, the term "*click data*" should apply to all user interaction data. ***In the second place*****,** even if a narrower interpretation to the term "*click data*" is applied, *quod non*, dwell time is a user interaction which is measured though a click as it concerns the time that passed from the moment the search results were presented to the user until the moment the user clicked on one of the results. ***In the third place*****,** information about the time a user spent viewing the search results and about the size and visibility of search results on the user's device also fall under "*view data*" as they concern the question whether and for how long the results served by the OSE were viewed, i.e., generated an impression.

(416) **Second**, applying the principle of parity requires the sharing of this data, which Alphabet itself collects for the purpose of optimising its OSE services. [Description of Alphabet's measurements of user interaction],[620][description of Alphabet's measurements of user interaction].[621] [Description of Alphabet's internal system processes and components],[622] [Description of Alphabet's measurements of user interaction].[623] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(417) **Third**, the data is required for OSE optimisation. Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as indicated in recital 61, such data should be covered by the obligation of Article 6(11) of Regulation (EU) 2022/1925. The time a user spent reviewing a

---

619 The text of the measure is repeated here for ease of reading, the binding text is provided in the Annex to this Decision.

620 Alphabet's reply to RFI10, Annexes Q1.2 and Q5 Doc IDs […]; Alphabet's reply to RFI10 follow-up, Annex Q1, Doc ID […].

621 [Direct quote describing Alphabet's internal system processes and components]. See Alphabet's reply to question 30 of EC RFI 2 dated 30 January 2026, Doc ID […].

622 [Direct quote describing Alphabet's internal system processes]. See Alphabet's reply to question 1(e) of EC RFI 8 dated 19 February 2026, Doc ID […].

623 Alphabet's reply to RFI10 follow-up, Annex Q1, Doc ID […]; Alphabet's reply to RFI10 Annex 14.3, Doc ID […]; Alphabet's reply to question 3 of EC RFI 8 dated 19 February 2026, Doc ID […].

search result reflects the level of attention given to the result and can serve as feedback on the relevance of the result to the user search. For certain types of results, such as direct answers and knowledge panels, a long dwell time represents the best feedback for the quality and relevance of the result, as it shows that they user found the answer to its query on the SERP itself and did not require to further engage with any other search results.

(418) ***In the first place***, this is supported by Alphabet's internal documents. For example, one of Alphabet's internal documents explains [description of Alphabet's measurement of user interaction]..[624] Another internal document of Google explains that "*a long look might mean a* [knowledge panel] *was interesting*".[625]

(419) ***In the second place***, this is confirmed by third parties. Market participants noted that "*comprehensive information on no-click impressions* […] *are essential for evaluating relevance and detecting spam*".[626] The average rating by market participants who replied to the Commission's RFI for the importance of dwell time to OSE optimisation was 4.2 on a scale from 1-5.[627] Market participants explained that the data is an "[e]*ssential satisfaction signal, including "no-click" queries where users stay on the SERP because the answer is shown directly. Needed to optimise relevance beyond positive clicks alone*",[628] and that it "[i]*ndicates whether users are satisfied with SERP content or continuing to search. Long SERP dwell times may indicate users comparing options or struggling to find relevant results*";[629]

(420) **Fourth**, for the reasons listed in recitals (380) to (384), the data should be shared for all search results, regardless of their type**.**

(421) **Fifth**, for the reason listed in recital (385), the data should be provided in a non-aggregated manner.

(422) **Sixth**, sharing this data would not allow copying of Alphabet's technologies, nor would it discourage innovation. Further to the reasons listed in recital (390), the measures do not require the sharing of the relevant time intervals that Alphabet uses as indicators of good or inferior quality and relevance of the search results, nor do they require the sharing of information on the type of results for which certain dwell time serves as positive indicator for user satisfaction. Alphabet is not required to specify what dwell duration, in its view, represents user's satisfaction and what dwell duration represents user dissatisfaction. Therefore, the data would not allow beneficiaries to understand how Alphabet encodes and interprets dwell time. Alphabet is only required to share dwell time or the raw data that would allow beneficiaries to calculate dwell time per SERP Element.

4.3.2.3.4. Hovering, scrolling, swipes and expansions

4.3.2.3.4.1. Introduction

(423) Hovering, scrolling, swipes and expansions are forms of user interaction. These are actions through which users navigate the SERP and revise content visibility on the SERP. Hovering refers to the movement of the user's mouse over a result. Scrolling

624 Alphabet's reply to RFI10 Annex 14.3, Doc ID […].

625 Document submitted as trial exhibit UPX0228 in U.S case 1:20-cv-03010-APM, Doc ID […]

626 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3;

627 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

628 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1, Doc ID […].

629 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1, Doc ID […].

and swiping can be done vertically or horizontally and can refer to the SERP itself or elements included in it. The existence or absence of these actions (and for hovering also duration), provide information on the content visible to the user and the user's attention to a given result and therefor the relevance of the results to its query.

(424) The Google Search Data does not include any information on any of these actions.

4.3.2.3.4.2. The Commission's assessment

(425) As set out in section 4.3.2.3.1.2, recitals (365)(c) to (365)(f), the Commission considers that to meet the requirements of Article 6(11) of Regulation (EU) 2022/1925 Alphabet must share with eligible third-party OSEs for each SERP Element: (i) the duration, or the absence of, hovering on the SERP Element; (ii) the number, or the absence of, scrolls on the SERP; (iii) the occurrence, or the absence of, swipes within a swipeable SERP Element, and (iv) the occurrence, or the absence of, expansion of a SERP Element.[630]

(426) Below, the Commission provides reasons, additional to those provided in section 4.3.2.3.1.4, as to why it is specifying these measures.

(427) **First**, the data falls under Article 6(11) Regulation (EU) 2022/1925. ***In the first place***, as explained in recitals (368) *et seq.,* above, the term "*click data*" should apply to all user interaction data. ***In the second place*****,** these data types clearly fall under the term "*click data*", as at least on mobile devices, there is not much difference between the actions of scrolling, swiping and expanding and the action of clicking on a result, as they are all performed through touching and taping the device's screen. As such, they closely resemble clicks and should be considered as "*click data*". In relation to expansions, Alphabet confirmed that expansions are tracked as click events on the expansion feature,[631] further demonstrating the resemblance of the actions to clicks and furthermore confirming that expansions also fall under click data due to the fact that they are measured through clicks. ***In the third place*****,** information about the duration a user hovered over a result and about user actions navigating the SERP through scrolling swiping and expansions also fall under "*view data*" as it concerns the attention given by the user to the result and the visibility of the search results on the user's device and therefore the question whether and for how long the results served by the OSE were viewed, i.e., generated an impression.

(428) **Second**, applying the principle of parity requires the sharing of this data, which Alphabet itself collects and uses for the optimisation of its OSE services. [Description of Alphabet's measurement of user interaction],[632] [description of Alphabet's measurement of user interaction].[633][Description of Alphabet's internal system processes and components],[634] [description of Alphabet's measurement of user interaction].[635] As explained in section 4.3.1, the Commission considers that the

630 The text of the measure is repeated here for ease of reading, the binding text is provided in the Annex to this Decision.

631 Alphabet's reply to question 3 of EC RFI 8 dated 19 February 2026, Doc ID […].

632 Alphabet's reply to RFI 10, Annexes Q1.2 and Q5, Doc IDs […]. Alphabet explained that [direct quote describing Alphabet's measurement of user interaction]. See Alphabet's reply to question 30 of EC RFI 2 dated 30 January 2026, Doc ID […].

633 Alphabet's reply to RFI10, Annexe Q5, Doc ID […]. Alphabet explained that [direct quote describing Alphabet's measurement of user interaction], see Alphabet's reply to question 30 of EC RFI 2 dated 30 January 2026, Doc ID […].

634 [Description of Alphabet's internal processes]. See Alphabet's reply to question 1(e) of EC RFI 8 dated 19 February 2026, Doc ID […].

635 Alphabet's reply to RFI 10 follow-up, Annex Q1, Doc ID […]; Alphabet's reply to questions 1 and 3 of EC RFI 8 dated 19 February 2026, Doc ID […].

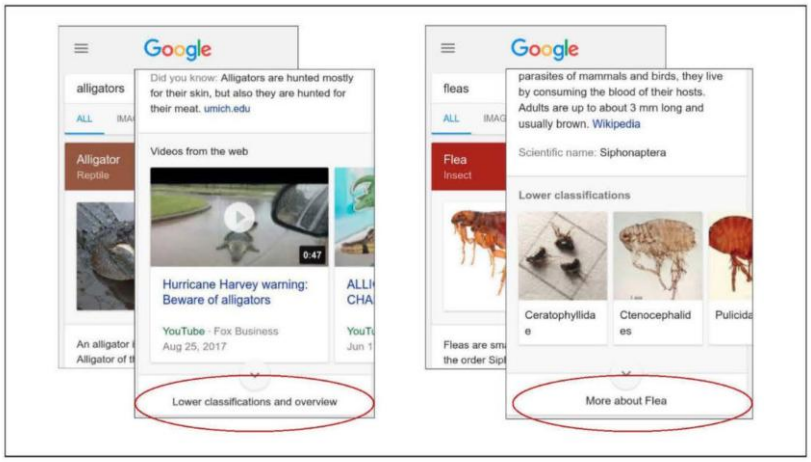
relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(429) **Third**, the data is required for OSE optimisation. Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as indicated in recital 61, such data should be covered by the obligation of Article 6(11) of Regulation (EU) 2022/1925. User actions hovering, scrolling swiping and expanding the SERP or element on the SERP reflect the level of attention given to these results and can serve as feedback on the relevance of the results to the user search. A long hover, or using navigational actions to expose more information available in a given result demonstrate the user's interest in the result. For certain types of results, such as direct answers and knowledge panels, such actions provide good feedback for the quality and relevance of the result despite the absence of a click, as they show that the user explored them in depth or that the user found the answer to its query on the SERP itself and did not require to further engage with any other search results. Information on scrolling provides information on the number of results viewed by the user and may indicate that results appearing higher on the SERP were of lower relevance as they did not satisfy the user. In addition, scrolling and swiping around specific results, as well is hover time below and above a given result can indicate an implicit impression and thus allows OSEs to identify more effectively the results that generated impressions.

(430) ***In the first place***, this is supported by Alphabet's internal documents. For example, one document explains that taping on a knowledge card to expand and fully open it provides important feedback on the type of information the user would like to see in response to the user's query and that it is therefore important to log these actions and endow them with meaning (see Figure 12 below). Another Alphabet document explains that [direct quotes and description of Alphabet's internal system processes and components].[636] [Direct quotes and description of Alphabet's internal system processes and components].[637] [Direct quotes and description of Alphabet's internal system processes and components]. [638]

636 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], pages 11-13.
637 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 13.
638 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 13.

Figure 12: Alphabet's internal document titled "Google is magical"



For example, some knowledge cards need an extra tap to fully open.
On the left, an extra tap means the user wants lower classifications and an overview.
On the right, the user has too little background information.
More what? How is tapping here different from scrolling down? Users can't make a good decision, so
Taps and clicks are such distinctive events in logs; we should endow every one with meaning.

Source: Document submitted as trial exhibit in U.S vs. Google[639]

(431) ***In the second place***, this is supported by third parties. A market participant noted that "*optimisation requires access to click data* […] *including* […] *scroll behaviour (both vertical and horizontal), which reflects result-set exploration and ranking adequacy; and expansions or other interactive actions on result modules, menus, or enriched UI elements.* [the market participant's] *general view is that these distinctions are usually critical for training and calibrating relevance, ranking, and answer-quality models."*[640] One market participant explained that "*Scrolling pattern help us to distinguish between passive tab-open behavior and active content exploration*";[641]

(432) The average rating by market participants who replied to the Commission's RFI for the importance of hover time to OSE optimisation was 3.4 on a scale from 1-5.[642] Market participants explained that hover time "*Indicates user consideration and interest even without clicking*";[643] "*Understanding the user's mouse behaviour will be an important function for spam behaviour*".[644] The average rating by market participants who replied to the Commission's RFI for the importance of scrolling patterns to OSE optimisation was 3.1 on a scale from 1-5.[645] Market participants explained that the data "C*an help interpret whether users explored result sets*",[646] and "[i]*ndicates user engagement with content and whether they explored beyond*

639 Trial exhibit UPX0228 in *case 1:20-cv-03010-APM,* Doc ID […].
640 [Market participant]'s reply to RFI 1 of 18 November 2025, tranche 2, Doc ID […], question 3.
641 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Doc ID […], question 7.
642 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].
643 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].
644 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].
645 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 of 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].
646 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

initial visible results. Shows depth of search and whether top results satisfied user need or they needed to scroll for alternatives".[647]

(433) **Fourth**, for the reasons listed in recitals (380) to (384), the data should be shared for all search results, regardless of their type.

(434) **Fifth**, for the reason listed in recital (385), the data should be provided in a non-aggregated manner.

(435) **Sixth**, sharing this data would not allow copying of Alphabet's technologies, nor would it discourage innovation. Further to the reasons listed in recital (390) above, the measures do not require the sharing of the way Alphabet uses information about hovering, scrolling, swiping and expansions, and what combination and duration of such actions is used as indicators of good or inferior quality and relevance of the search results. Therefore, that data would not allow beneficiaries to understand how Alphabet encodes and interprets hover duration, scrolling patterns, swipes and expansions. In particular, Alphabet is only required to share the raw data on the existence of these actions and their impact on the content visible on the user's SERP.

4.3.2.4. Ranking data

(436) This section presents the considerations of the Commission on the specified measures and the reasons for them in relation to ranking data. Section 4.3.2.4.1 provides an introduction of ranking data; section 4.3.2.4.2 sets out the specified measures the in relation to ranking data, section 4.3.2.4.3 provides the summary of gatekeeper's view, and section 4.3.2.4.4 provides the Commissions' assessment underpinning the measures.

4.3.2.4.1. Introduction

(437) The way search results are organised and displayed on the SERP affect the users' perceived relevance of these results and, consequently, the way users engage with these results. Information concerning the way search results are organised and displayed on the SERP therefore provides important context to the data concerning users' engagement with these results. Such data is necessary for the optimisation of OSE services.

(438) The Google Search Data includes, for each organic result separately and for advanced search results blocks, the search result's average rank over a three-month period, where for the calculation of the average rank, organic results are considered individually, and advanced search results are considered as blocks.[648]

(439) For the reasons listed in section 4.3.2.4.4, the Commission is specifying the measures included in section 4.3.2.4.2.

4.3.2.4.2. Measures

(440) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, subject to anonymisation requirements, for each SERP Element shared pursuant to the paragraphs concerning view data of these measures, Alphabet must share with eligible third-party OSEs (i) the SERP Element's absolute, whole page position on the SERP as displayed on the user's device, (ii) the SERP Element's relative ordinal position, in relation to other SERP Elements presented within the same area on the SERP and (iii) any other information on the SERP Element's relative and absolute

647 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

648 Alphabet's reply to RFI 1 of 28 November 2023, Doc ID […], question 7, paragraph 28, and question 9, paragraphs 33-34.

position, prominence and visibility on the SERP, as displayed on the user's device, on par with the data collected by Alphabet for the purpose of optimising its OSE service.

(441) It follows that Alphabet must share with eligible third-party OSEs at least the following ranking data for each SERP Element shared pursuant to the paragraphs concerning view data of these measures:

(a) Identifier of the absolute, whole page position on the SERP in which the SERP Element is displayed (e.g., top area, main column, right side column);

(b) The relative ordinal position of the SERP Element in relation to other SERP Element displayed in the same SERP area and the identification of all other SERP Elements displayed in the same area;

(c) Information about the page on which the SERP Element was displayed on the user's device;

4.3.2.4.3. The gatekeeper's view

(442) In its response to the Preliminary Findings, Alphabet did not refer specifically to the measures concerning ranking data. However, some of Alphabet's general claims[649] refer, among others, to ranking data. Alphabet claims that the measures, including the sharing of detailed ranking data, expropriate the value from Alphabet generating processing and organizing its data,[650] as well as Alphabet's innovation, work and investment in developing its algorithms and indexing systems,[651] because, according to Alphabet, recipients would be able to copy the output of Alphabet's algorithms,[652] imitate Alphabet's algorithms[653] and freeride Alphabet's costly innovations and investments.[654] Alphabet further argues, that this expropriation conflicts with the DMA objectives.[655]

4.3.2.4.4. The Commission's assessment

(443) The Commission is specifying the measures listed in section 4.3.2.4.2 for the following reasons.

(444) **First**, ranking data should be interpreted to include all information concerning the way the search results were presented to the user. Article 2(22) of Regulation (EU) 2022/1925 defines ranking broadly, referring to the relative prominence or relevance given to the search results as presented, organised or communicated by the OSE: "***the relative prominence*** *given to goods or services offered through online intermediation services, online social networking services, video-sharing platform services or virtual assistants,* ***or the relevance given to search results by online search engines, as presented, organised or communicated*** *by the undertakings providing online intermediation services, online social networking services, video-sharing platform services, virtual assistants or online search engines, irrespective of the technological means used for such presentation, organisation or communication and irrespective of whether only one result is presented or communicated*" [emphasis added]. The relevance of results as presented organised or communicated should be interpreted to apply to all information relating to the position and relative position on

649 The Commission deals with these claims more in detail in section 4.3.1 of this Decision.
650 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 28-34.
651 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 35-39.
652 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 40-50.
653 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 51-55.
654 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 56-64.
655 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraphs 65-67.

the SERP. This includes at least the position of a result on the SERP, its ordinal position and the page in which it is presented.

(445) **Second,** ranking data should be shared in a non-aggregated manner, meaning that rather than the average ranking per result, Alphabet should share the explicit ranking and position information of each SERP Element served in response to each user query. In addition, ranking data should be provided as visible on the user's device and not aggregated across devices.

(446) ***In the first place***, there is nothing in Regulation (EU) 2022/1925 to suggest that the ranking information should be provided as an average. As explained above, Regulation (EU) 2022/1925 defines ranking broadly rather than narrowly, and an interpretation requiring only average ranking would narrow it down without justification. The regulation should therefore be understood as referring to the actual way in which the search results were organised and presented.

(447) ***In the second place***, providing average, rather than explicit ranking information conceals extremes and does not provide the contextual information required to evaluate users' engagement with the results. Providing ranking data in an aggregated manner does not allow beneficiaries to know the position of the SERP Element on the SERP when the SERP Element was viewed or clicked. In addition, aggregated ranking does not allow beneficiaries to understand which results were displayed close to the clicked result. In this respect, one market participant explained that "[a]*veraging hides extremes, for example, a URL that appears equally often in the first and the tenth position over three months would be reported with an average rank of five—but links in the first position appear at the top of a page, and links in the tenth position appear at the bottom of a page*";[656] Another market participant explained that "*While an aggregate result* […] *is useful, it is distorted and does not provide holistic ranking information. An average position can appear stable even when individual users see wildly different results*. […] *Search quality and fairness are often judged by worst-case and best-case experiences. For example, knowing that a domain appears at position 1 for some users but drops to position 40 for others is far more actionable than an average of 12* […]";[657] The market participant further explains, in relation to aggregation across devices, that "*Aggregating* [ranking] *data across devices hides important differences in layout, visibility, and user behaviour*" and noted that "*the same position can have very different visibility on mobile versus desktop*";[658]

(448) ***In the third place***, given that due to the anonymisation requirements, no URLs will be provided for paid search results (see section 4.4.4.1), the Commission considers that sharing ranking data for anonymised paid search results, will not disclose sensitive commercial information of Alphabet and third-party advertisers.

(449) **Third,** ranking data should be shared for all search results, regardless of their type.

(450) ***In the first place***, Article 6(11) of Regulation (EU) 2022/1925 requires the provision of ranking, query, click and view data "*in relation to free and paid search*". Article 2(23) of the Regulation further clarifies that "*'search results' means any information in any format, including textual, graphic, vocal or other outputs, returned in response to, and related to, a search query, irrespective of whether the information*

656 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3. See also [Market participant]'s reply to RFI1 PO of 28 January 2026, Doc ID […], question 1, explaining that "*Position and Rank Information disappear when data is aggregated".*

657 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Doc ID […], question 6.

658 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Doc ID […], question 6.

returned is a paid or an unpaid result, a direct answer or any product, service or information offered in connection with the organic results, or displayed along with or partly or entirely embedded in them".

(451) ***In the second place***, Alphabet confirmed that it collects ranking data for all types of search results, including organic, advanced and paid search results.[659] The principle of parity therefore requires Alphabet to share this data with third party beneficiaries. [Description of Alphabet's use of data]. As explained in section 4.3.1.3 of this Decision, the Commission considers that the display of paid search results on the SERPs constitutes part of OSE services. Therefore, the fact that Alphabet collects and uses user data related to paid search results for optimising the presentation of search ads on the SERPs amounts in Alphabet colleting this data for the purpose of optimising its OSE services and it is sufficient for the inclusion of this data in compliance with the parity principle. As explained in section 4.3.2.2.3 above, paid search results constitute a substantial part of the SERP. The definition of '*search results*' in Article 2, point (23), of Regulation (EU) 2022/1925 confirms that paid search results returned in response to a user query form part of the online search engine services. [Description of Alphabet's use of data], should not mean that third parties must also be prevented from using this data in relation to paid search results when optimising their online search engine services.

(452) ***In the third place***, to understand the user's intent based on the user's interaction with the SERP, an OSE has to know everything the user saw. Excluding ranking data for some of the elements presented to the user creates blind spots that may distort OSE's understanding of the user interaction data. This is supported by views of market participants, who explain, for example, that "*user clicks and behaviour on results are directly influenced by the presence and position of ads. Without ads URLs, any modelling of SERP layout or user interaction patterns is incomplete.* […]*Without knowing which ads were present, click-through patterns on organic results appear artificially distorted*";[660] "*advanced units above organic results* […] *strongly influence click behaviour"*;[661] "[V]*isibility into ads URLs at the view level may generally help OSEs understand the full context in which users interact with a search results page, including how the presence, placement, and format of ads affect user attention, scrolling behaviour, and engagement with organic results*";[662] "[the market participant]*'s general perspective is that advanced search URL links can help optimise an OSE. Without visibility into these advanced result formats, an Alphabet rival's optimisation process would be biased toward "blue-link-only" results and would fail to accurately interpret user behaviour on pages where a substantial share of user satisfaction occurs without any clicks*";[663] "*A user's engagement is impacted by results shown relative to each other and the ranking of results just within their own grouping is not useful. As such, it is essential to understand the overall ranking order of all results holistically*".[664]

(453) **Fourth,** applying the principle of parity requires the sharing of this data, which Alphabet itself collects and uses for the optimisation of its OSE services. [Description of Alphabet's internal system processes and components].[665] As

---

659 Alphabet's reply to Alphabet's reply to RFI 2 of 22 December 2023, Doc ID […], question 38.

660 [Market participant]'s reply to RFI 2 of 18 November 2025, Doc ID […], question 6.

661 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

662 [Market participant]'s reply to RFI 1 of 18 November 2025, tranche 2, Doc ID […], question 6.

663 [Market participant]'s reply to RFI 1 of 18 November 2025, tranche 2, Doc ID […], question 9.

664 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

665 Alphabet's reply to RFI 10 of 12 November 2025, Annexes Q1.2 and Q14.3, Doc ID […] Alphabet's reply to RFI 10 follow-up of 12 November 2025, Tranche 1, Annex Q1, Doc ID […].

explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, and considering that this data is required for OSE optimisation (as explained in the subsequent recitals), Alphabet's access to this data forms part of the barrier to entry and expansion undermining contestability of online search engines, identified in recital 61 of the Regulation, and the data should therefore be shared with third parties.

(454) **Fifth,** the data is required for OSE optimisation. Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as indicated in recital 61, such data should be covered by the obligation of Article 6(11) of Regulation (EU) 2022/1925. The position on the SERP and the order in which search results are displayed affect the perceived relevance of these results to the user's search and, consequently, users' actions interacting with the search results. Detailed information about the absolute and relative position of search results with which the user engaged therefore provides crucial context to the engagement data, as it allows the OSE to interpret the user engagement data and assess to what extent the user engagement indicates that users considered the result relevant to their query. For example, user engagement with results which are positioned lower on the SERP carries more weight than user engagement with the first result on the SERP, which may have been driven by position bias. The relative position of search results can also be used to identify the results viewed by the user, for example if they were positioned above a result with which the user engaged. User engagement with a certain result may carry feedback on their relevance to the user query also in relation to other results which were presented in vicinity to that result. It can indicate their relevance (e.g., when the result is part of the same block) or irrelevance (e.g., when a result right above the result with which the user engaged does not get clicked).

(455) ***In the first place***, this is confirmed by Alphabet's internal documents. [Description of Alphabet's measurement of user interaction];[666] [Description of Alphabet's measurement of user interaction];[667] [Description of Alphabet's measurement of user interaction].[668] Alphabet's internal documents further [description of Alphabet's measurement of user interaction].[669]

(456) ***In the second place***, this is confirmed by third parties. Market participants consider data on the *rank/ order* of results returned in response to each query to be essential to OSE optimisation: the average rating by market participants who replied to the Commission's RFI for the importance of the *rank/ order* of results to OSE optimisation, on a scale from 1 to 5, was 5.[670] Market participants further consider that data concerning the *position* of search results on the page is very important for OSE optimisation, and on average have rated its importance to be 4 on a scale from 1-5.[671] Market participants considered ranking data for *advanced* and for *paid search results* to be similarly important to OSE optimisation: The average rating by market

666 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.7, Doc ID […], page 17.

667 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, Doc ID […], page 13.

668 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.5, Doc ID […], page 22.

669 Alphabet's reply to RFI 10 of 12 November 2025, Annex 14.3, page 9, Annex 14.5, slide 28.

670 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

671 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1 (Doc ID […]).

participants who replied to the Commission's RFI for the importance of this data to OSE optimisation on a scale from 1-5 was 4.6 for advanced search results and 4.3 for paid search results.[672] Market participants explained that rank and order data is a "[c]*ore input for understanding ranking decisions and relevance outcomes"*;[673], that "*Screen position affects visibility and clicks and supports meaningful optimisation analysis*";[674] that "*Actual position affects user behavior and click likelihood*";[675] and that "*without understanding where results appear on the search results page, it is not possible to interpret user interaction patterns accurately*".[676] One market participant provided its general observation that *"without knowing how results were ranked and ordered at the time they were shown to users, it is unlikely that view or click behaviour could be interpreted accurately*. [The market participant]*'s general view is that ranking data would typically be required for OSEs to: evaluate whether user engagement patterns reflect true relevance or are driven by position bias; train and validate ranking models that predict the optimal ordering of results for different queries, users, and contexts; and measure the impact of changes to ranking logic over time by comparing user behaviour against known baselines*";[677] Another market participant referred to the position/rank of the URL when it was clicked as a "*crucial signal*", explaining that a "*click on a lower-ranked result is a more powerful relevance signal than a click on a higher-ranked result, because users tend to click lower-ranked links less frequently due to their position, not just their relevance*".[678] The market participant further explained that the "*layout of the SERP* […] *lets us calculate how much (vertical) space each result takes up, the order of results, which results are initially off-screen, and how far the user has to scroll to see these results*. […] *Ranking and actual position on a SERP are different but both of fundamental importance. For example, if you search for a well-known celebrity, the top of the page might be dominated by image results, which would put the number 1 ranking organic URL result much lower down the page than it might otherwise be*";[679] According to the market participant, this data is used, among others, "*to normalize click rates*" as users are more likely to click on "*results higher up the page"; "results that take up more vertical space on the page", and "results that are visible without scrolling*".[680]. In relation to ranking data for advanced and paid search results, market participants explained that "*Advanced modules materially shape user behaviour and require ranking transparency*";[681] that "*Module positioning affects visibility and clicks*";[682] and that "*user clicks and behaviour on results are directly influenced by the presence and position of paid search results. Without seeing the ranking data for paid search URLs, any modelling of SERP layout or user interaction patterns is incomplete*".[683]

672 Where 1= not important, 2= low importance, 3=moderately important, 4= very important, 5=essential. See replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

673 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

674 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

675 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID 1[…].

676 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

677 [Market participant]'s reply to RFI 1 of 18 November 2025, tranche 2, Doc ID […], question 3.

678 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

679 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Doc ID […], question 10.

680 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Doc ID […], question 10.

681 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

682 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

683 [Market participant]'s reply to RFI 1 PO of 28 January 2026, Annex 1, Doc ID […].

(457) **Sixth,** sharing this data would not expropriate Alphabet's intellectual property and innovation, or allow copying of Alphabet's technologies, nor would it discourage innovation. Any reliance of the measures on Alphabet's effort or innovation does not go beyond what was intended for by the legislator.

(458) ***In the first place***, the measures do not require the sharing of ranking algorithms nor of ranking signals, but rather data shown following user searches and seen by users, that would allow third party OSEs to develop ranking signals of their own. In particular, the measures do not require Alphabet to share the reasons or the technology that led to a certain result being displayed higher or lower on the SERP. They only require sharing the final position of the results as displayed on users' devices. This data would not reveal, and therefore not allow the copying of Alphabet's ranking algorithms.

(459) ***In the second place***, according to Alphabet itself, its ranking algorithms are very complex, and rely on many signals, [description of Alphabet's internal systems] but rather on Alphabet's own efforts. [Direct quotes describing Alphabet's internal system processes].[684]

(460) ***In the third place***, all market participants who provided a non-confidential reply to the Commission's question about the possibility to infer the types and values of different signals used by Alphabet's search and ranking algorithms from click, query, view and ranking data shared by Alphabet confirm that they do not consider it would be possible.[685] One market participant noted that "*modern search ranking systems are not governed by simple rules or fixed weights, and that access to external query, view, click, or ranking-position data does not enable recovery of internal ranking formulas, signal weights, proprietary feature definitions, or model architectures*".[686]

(461) ***In the fourth place***, the information about how search results were organised and displayed on the SERP is not confidential to Alphabet, considering that it was shared with the users. Theoretically, the way search results were organised and displayed could be replicated by conducting a similar search under similar conditions.

(462) ***In the fifth place***, as explained in section 4.3.1, granularity and completeness of the data to be shared pursuant to these measures will be reduced due to anonymisation requirements, which will further limit recipients' ability to copy or imitate Alphabet's algorithms and their output. In addition, due to the anonymisation requirements and technical limitations, data will be shared with a significant latency of no less than seven days (see sections 4.3.3.2 and 4.4), thus preventing recipients from simply copying the output of Alphabet's algorithms as described by Alphabet. The measures also specifically prohibit the mere copying by recipients of search results directly from the dataset (see section 4.4.4.2). Finally, the eligibility requirements set in the measures, as well as the audit requirements and the limited duration of the data sharing serve to ensure that eligible third party OSEs have sufficient incentive to innovate, rather than freeride Alphabet's efforts.

(463) ***In the sixth place***, as explained in section 4.3.1 above, by requiring the sharing of, among others, ranking data, the legislators' intention was to foster innovation in search services. To the extent the sharing of ranking data with eligible third party OSEs make use of Alphabet's innovation (as argued by Alphabet), this was the

---

684 Alphabet's reply to RFI 8 of 22 July 2025, Doc ID […], question 10.

685 Replies of market participants to question 10 of RFI of 18 November 2025, Doc ID […]; Reply of a market participant to RFI of 17 February 2026, Doc ID […], question 11.

686 [Market participant]'s reply to RFI 1 of 18 November 2025, tranche 2, Doc ID […], question 10.

legislator's choice, and the measures do not require sharing any data that goes beyond the legislators' choice.

4.3.3. Conditions of data sharing

(464) This section presents the considerations of the Commission on the specified measures and the reasons for them in relation to conditions of data sharing, setting out that invalid traffic should be excluded from the data shared pursuant to Article 6(11) of Regulation (EU) 2022/1925 (section 4.3.3.1); as well as the required latency, batches, time stamps (section 4.3.3.2), method (section 4.3.3.3) and duration (section 4.3.3.4) of data sharing. Each section provides an introduction of the topic, the measures and the Commission's assessment underpinning the measures. Finally, consideration in relation to search session data are provided (section 4.3.3.5).

4.3.3.1. Invalid traffic

4.3.3.1.1. Introduction

(465) "**Invalid traffic**" is interaction (e.g., queries, impressions and clicks) which is not genuine human traffic, or that does not come from a genuine user interest, such as traffic that is believed to be machine generated, fraudulent or spam like.[687] As such, it is not a useful source for assessing search results' relevance to users' queries and, if used, may distort OSE services optimisation.

(466) Queries that are blocked by Google's systems because they are identified as not originating from a human user and therefore do not trigger a results page are not included in Alphabet's European Search Dataset Licensing Program.[688] However, if a query triggers a results page, the Dataset does not exclude clicks based on Google's mechanisms for detecting click spam (i.e., "invalid traffic"),[689] meaning that click data as reported in the Dataset may include invalid traffic. The Dataset does not include any invalid traffic identifiers.[690]

(467) For the reasons listed in section 4.3.3.1.4, the Commission is specifying the measure included in section 4.3.3.1.2.

4.3.3.1.2. Measure

(468) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925 Alphabet must exclude invalid traffic, i.e. query, view, click and ranking data, that does not originate from a human user or a genuine user interest, from the Search Data shared with eligible third-party OSEs. To exclude invalid traffic, to the extent technically possible, Alphabet must use the same methods and process it uses itself in its ordinary course of business and must not give rise to incremental costs attributable to making the data available.

(469) Alphabet must provide, upon request of eligible third-party OSE information enabling the third party to understand how invalid traffic is excluded and how the exclusion of invalid traffic impacts the dataset, without revealing Alphabet's business secrets.

---

687 The term spam also refers to web pages using various tactics to achieve high ranking by OSEs despite their low-quality content. Invalid traffic is one of the tactics used to improve the web page ranking by OSEs. This section covers only the identification of user-side actions, i.e. the queries, clicks, and other user interactions as invalid, and not the data concerning the identification of a certain webpage as spam.

688 Alphabet's reply to RFI 8 of 22 July 2024, Doc ID […], question 4.

689 Alphabet's reply to RFI 8 of 22 July 2024, Doc ID […], question 4.

690 Alphabet's compliance report 2024, paragraph 107; Compliance report 2025, paragraph 97.

4.3.3.1.3. The gatekeeper's view

(470) In its response to the Preliminary Findings, as part of its general claim that the measures expropriate the value from Alphabet's generating, processing and organizing its data,[691] Alphabet notes that its spam filtering systems are the product of Alphabet's significant intellectual efforts and investments.[692] Separately, Alphabet submits that the requirement to remove invalid traffic from the dataset shared with eligible third party OSEs, combined with a high sharing frequency, would enable recipients to "*reverse-engineer and defeat Google's anti-scraping protections*".[693]

(471) In its response to the Revised Measures, Alphabet argues that, together with other reporting obligations, the measure requiring it to inform eligible third party OSEs how invalid traffic is excluded and how the exclusion of invalid traffic impacts the dataset, outsources the Commissions' monitoring task to third parties.[694] To the extent any disclosure is necessary, Alphabet submits it should be made to the Commission.[695] In addition, Alphabet claims that considering that the measure does not require disclosure of business secrets, it is difficult to see what information third parties could receive or why they would need such information.[696] Alphabet also argues that it is not clear why third parties would need this information for optimizing their search engines. [697]

4.3.3.1.4. The Commission's assessment

(472) **First**, invalid traffic does not form part of the data covered by Article 6(11) of Regulation (EU) 2022/1925 and should therefore be excluded from the data shared by Alphabet. ***In the first place***, Article 6(11) of the Regulation requires the sharing of "*ranking, query, click and view data* […] *generated by end users*". According to Article 2(20) of the Regulation, "*'end user' means any natural or legal person using core platform services other than as a business user*". Invalid traffic which does not originate in a genuine end user, should therefore be excluded from the dataset. In this respect, Alphabet itself defines invalid traffic as "*any activity that doesn't come from a real user with genuine interest. It can include accidental clicks caused by intrusive ad implementations, fraudulent clicking by competing advertisers, advertising botnets and more*."[698] ***In the second place***, Alphabet itself agrees with the principle of excluding data which does not originate from real users. Alphabet explained that "*Queries that are not issued by real users are beyond the scope of Art. 6(11) and do not serve the purpose of this provision*".[699] The Commission notes that Alphabet's approach, that "*[i]f a query triggers a results page, Google reports all clicks on that page. Google does not exclude clicks or views based on its mechanisms for detecting*

691 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 28-34.
692 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 32 (c).
693 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 393.
694 Alphabet's response to the Revised Measures, Doc ID […], paragraph 102.
695 Alphabet's response to the Revised Measures, Doc ID […], paragraph 102(a).
696 Alphabet's response to the Revised Measures, Doc ID […], paragraph 102(a).
697 Alphabet's response to the Revised Measures, Doc ID […], paragraph 102(a).
698 See: https://www.google.com/ads/adtrafficquality/invalid-activity/, last visited on 10 April 2026, Doc ID […]; Alphabet defines invalid traffic similarly in various instances, for example: "*Invalid traffic refers to clicks and impressions on ads that aren't a result of genuine user interest, including intentionally fraudulent traffic and accidental or duplicate clicks*.", see: https://support.google.com/google-ads/answer/11182074?hl=en, last visited on 10 April 2026, Doc ID […]); " *Invalid traffic includes any clicks or impressions that may artificially inflate an advertiser's costs or a publisher's earnings. Invalid traffic covers intentionally fraudulent traffic as well as accidental clicks*", see: https://support.google.com/adsense/answer/16737?hl=en, last visited on 10 April 2026, Doc ID […].
699 Alphabet's reply to RFI 3 of 23 February 2024, Doc ID […], Table 1.

click spam (i.e., "invalid traffic") when generating the click and view data reported in the Art. 6(11) Dataset",[700] appears contradictory to Alphabet's view stated above. ***In the third place***, the fact that Alphabet uses its proprietary technology to identify invalid traffic does not justify the inclusion of invalid traffic in the data shared with third parties, as it is not part of the data covered by Article 6(11) of the Regulation.

(473) **Second,** invalid traffic is not useful for OSE services optimisation and using it for OSE services optimisation may distort the optimisation process as it provides distorted user feedback on the quality and relevance of search results to the user's query. [Description of Alphabet's internal system processes].[701] Third parties also confirm that invalid traffic is not useful to assess search results' relevance.[702] Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as indicated in recital 61, such data should be *excluded* from the obligation of Article 6(11) of Regulation (EU) 2022/1925.

(474) **Third**, applying the principle of parity requires the exclusion of invalid traffic, [description of Alphabet's internal system processes and components].[703] [Description of Alphabet's internal system processes and components],[704] [description of Alphabet's internal system processes and components].[705] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself excludes such data for the purpose of optimising its OSE services, and considering that this data should be excluded for OSE optimisation (as explained above), the data should be excluded from the data shared with third parties.

(475) **Fourth**, third parties will likely not have the required data to identify invalid traffic based on the data included in the dataset. [Description of Alphabet's internal system processes],[706] but are not shared by Alphabet pursuant to Article 6(11) of the Regulation.

(476) **Fifth,** the exclusion of invalid traffic must be done, to the extent technically possible, using the same methods and process Alphabet uses itself in its ordinary course of business to exclude invalid traffic. ***In the first place***, this will ensure that Alphabet does not exclude traffic beyond or below what is necessary. As explained in recital (474), Alphabet excludes invalid traffic from the data used by its algorithms. Alphabet stresses on its websites the fact that it protects its advertisers and users from invalid traffic: "*Our Ad Traffic Quality team is dedicated to stopping all types of invalid traffic so that advertisers don't have to pay for it and the people who cause it don't profit from it*";[707] "*Invalid traffic is detected by Google's sophisticated monitoring systems. They can help you review, identify, and act on invalid clicks and impressions. You won't be charged for invalid clicks or impressions as they provide little or no value*",[708] and "*If we observe high levels of invalid traffic on your account, we may suspend or close the account to protect our advertisers and*

---

700 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID […], question 3.

701 Alphabet's reply to RFI 8 of 19 February 2026, Doc ID […], question 6.

702 See: [market participant]'s comments on Google's Digital Markets Act Article 6(11) Compliance proposal, 17 January 2024, Doc ID […], page 3.

703 Alphabet's reply to RFI 10 of 12 November 2025, Annex Q1.2, Doc ID […].

704 Alphabet's reply to follow-ups to RFI 10 and 11 of, Tranche 2, Annex Q1, Doc ID […].

705 Alphabet's reply to RFI 8 of 19 February 2026, Doc ID […], question 5.

706 Alphabet's reply to RFI 8 of 19 February 2026, Doc ID […], question 5.

707 https://www.google.com/ads/adtrafficquality/invalid-activity/, last visited on 10 April 2026, Doc ID […].

708 https://support.google.com/google-ads/answer/11182074?hl=en, last visited on 10 April 2026, Doc ID […].

users".[709] By requiring Alphabet to apply the same methods and process it uses itself to exclude invalid traffic from the dataset, the measures ensure that Alphabet excludes from the dataset the same traffic it identifies as invalid for the benefit of its own users and advertisers, and does not over exclude traffic that may otherwise be useful for OSE optimisation, or under exclude invalid traffic which is not useful for OSE optimisation. In this respect, several respondents to the Public Consultation highlighted the risk of over exclusion of traffic falsely identified as invalid from the dataset, or of under exclusion of invalid traffic.[710] ***In the second place***, requiring Alphabet to apply the same methods and process for the exclusion of invalid traffic addresses a clarification request by Alphabet. In an email to the Commission of 6 May 2026, Alphabet requested a clarification of reference in the measure to "*a genuine user interest*", stating it "*has no way of telling whether a query reflects a genuine user interest, or is entered by a user e.g. accidentally or in jest*."[711] The Commission considers that the reference to a genuine user interest is sufficiently explained in recital (465), which provides that examples for such traffic include traffic that is believed to be machine generated, fraudulent or spam like. The Commission also notes that, as explained in recital (472), Alphabet itself refers to "*activity that doesn't come from a real user with genuine interest*" when referring to invalid traffic. Nonetheless, the Commission considers that requiring Alphabet to apply the same methods and process for the exclusion of invalid traffic further clarifies that Alphabet should apply the same standard it applies in its usual course of business, as reported by Alphabet itself on its webpages. ***In the third place***, applying the same process Alphabet uses in its ordinary course of business will prevent replication of the process and generation of unnecessary and unjustified increase of the incremental costs attributed to making the data available. ***In the fourth place***, only to the extent the application of the same methods and process for the exclusion of invalid traffic are technically not possible, Alphabet may deviate from applying the same methods and process. Any deviation from the rule should be duly justified by exceptional limitation of technical nature.

(477) **Sixth,** the methods used to exclude invalid traffic and the impact on the dataset should be explained to beneficiaries in a meaningful and comprehensive manner, without revealing Alphabet's business secrets. ***In the first place***, this will allow beneficiaries informed use of the dataset. ***In the second place***, the obligation to share this information would further ensure that Alphabet makes only justified exclusion of invalid traffic and does not over exclude data which is otherwise useful for OSE optimisation. In this respect, several respondents to the Public Consultation highlighted the need for transparency in relation to the exclusion of invalid traffic.[712] ***In the third place***, third party OSEs interested in accessing the dataset are the appropriate addressees for such information. Such information can inform their decision to acquire access to the dataset and as operators of OSE they would be able to assess the validity of the exclusion and its impact on the dataset. In any case, the Commission can request Alphabet to share with it any such data as part of its investigative, enforcement and monitoring powers.

(478) **Seventh,** the measures would not allow copying of Alphabet's technologies, nor would it discourage innovation. ***In the first place***, as Alphabet is required to exclude

---

709 https://support.google.com/adsense/answer/16737?hl=en, last visited on 10 April 2026, Doc ID […].

710 See the following replies to the public consultations: [third party], Doc ID […]; [third party] Doc ID […].

711 Alphabet did not repeat this claim in its Response to the Preliminary Findings.

712 See the following replies to the public consultations: [market participant], Doc ID […]; [third party] Doc ID […]; [third party], Doc ID […].

invalid traffic from the dataset, beneficiaries will not have any visibility on the data excluded from the dataset and therefore on the technologies used to exclude it from the dataset. ***In the second place***, the measures do not require the sharing of the code used by Alphabet to identify the data as invalid traffic, nor do they require Alphabet to share the elements used to identify invalid traffic and weight given to each of them. This measure would not reveal, and therefore not allow the copying of Alphabet's algorithms. ***In the third place***, several aspects of the measures will together further prevent misuse of the dataset to learn about Alphabet's technologies for invalid traffic detection and will therefore address concerns raised by Alphabet [713] and by third parties[714] that the exclusion of invalid traffic combined with a high frequency of data sharing would allow to defeat Alphabet's anti-spam mechanisms in order to scrape and copy Alphabet's search results. The data will be shared with a significant latency of no less than seven days, thus creating a significant lag between any alleged attempts to bypass Alphabet's spam filtering and getting visibility as to the results of such attempts. In addition, the eligibility requirements set in the measures, as well as the audit requirements and the limited sharing duration serve to ensure that eligible third party OSEs have sufficient incentive to use the data for the purpose of optimising their OSE rather than for scraping and copying Alphabet's search results. Finally, the contractual measures set that third-party OSE will be required to use the Search Dataset solely for the permitted uses of optimising or improving OSE services and will be prohibited from using the Search Dataset for other unrelated uses.

4.3.3.2. Latency, batches and time stamps

4.3.3.2.1. Introduction

(479) "*Latency*" refers to the time intervals at which the Search Data should be shared by Alphabet with third parties. The "*freshness*" of data is an important aspect for the optimisation of search technologies, as it determines how reactive search services are to the changing web content. Latency is a different concept than batches and time resolution. A "*batch*" refers to the amount of time covered by one release or processing cycle, for example, a daily batch may contain all activity that occurred from midnight to midnight.[715] "*Time stamps*" (or time resolution), by contrast, refers to the precision with which the timing of events is recorded in the data itself. For example, in a daily batch, each query event can be recorded with a granularity of seconds, hours or a date (e.g., 30 May 2026).[716]

(480) The Google Search Data is made available to third parties on a quarterly basis, so every three months, and at the end of the succeeding quarter.[717] This means that, for example, Q1 data is shared with third parties at the end of Q2. The average latency between a user entering a query and the search data related to that query being disclosed to a third party is 4.5 months.[718] The Google Search Data comes in quarterly batches and does not include the time stamp.[719] Alphabet aggregates the

---

713 Alphabet's Response to the Preliminary Findings, Doc ID [...], paragraph 393.

714 See the following replies to the public consultation responses: [market participant], Doc ID […]; [third party], Doc ID […]; [third party], Doc ID […].

715 Alphabet's presentation of 7 May 2026, Doc ID [...], page 3.

716 Alphabet's presentation of 7 May 2026, Doc ID [...], page 3.

717 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 21.

718 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 2.

719 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 7.

data for the period of three months and does not distinguish when during that time frame the query was entered by the end user.[720]

4.3.3.2.2. Measures

(481) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must share the Search Data with eligible third-party OSEs on par with Alphabet's own latency of accessing the same data for the purpose of optimising its OSE services to the greatest extent that is technically feasible. The sharing of Search Data must be carried out within a timeframe of no less than 7 days, which reflects the minimum time technically needed [description of Alphabet's internal processes]to process the data, [description of Alphabet's internal system processes], and some additional days to anonymise and share the data with third-party OSEs. The final latency of Search Data sharing must be communicated by Alphabet within the time limit specified in section 4.6 to the Commission, along with a detailed technical description and justification why it is the lowest latency that can be technically achieved (including meaningful and comprehensive information that can be shared and tested with interested third parties without revealing business secrets, and subsequently notified to them).

(482) No matter the final latency, Alphabet must share the Search Data in daily batches and with daily time stamps.

4.3.3.2.3. The gatekeeper's view

(483) Alphabet argues that the real-time or high latency of data sharing measures that the Commission proposed in the Preliminary Findings (i.e., daily) is excessive.

(484) First, it has no legal basis in Article 6(11) of Regulation (EU) 2022/1925 which should expressly refer to "*continuous and real-time*" data access.[721]

(485) Second, it cannot be derived from the contested principle of parity.[722] Even if Article 6(11) of Regulation (EU) 2022/1925 provided for a parity obligation, the disclosure of data in real or near real-time would not be required, as the relevant reference point is [internal timeframe] with which Google accesses its data for optimising its search algorithms.[723] Alphabet continues that third-party OSEs confirm that algorithm training can be done based on historical data and based on granular time stamp rather than fresh data.[724]

(486) Third, Alphabet argues that the high latency of data sharing is disproportional as it harms Google, its users, and third-party websites.[725]

(487) Fourth, Alphabet argues that the real-time or high latency of data sharing are not technically practicable.[726] [Description of Alphabet's internal processes and system timeframes]. [727]

(488) Fifth, Alphabet points out that the parity principle as applied in relation to the latency for data access differs from its application in relation to query, view, click and

720 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 2b.
721 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 320-326.
722 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 327-347; Alphabet's submission dated 15 July 2026, Doc ID [...], paragraph 55.
723 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 348-363; 370-375.
724 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 364-369; 376-387.
725 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 389.
726 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 416.
727 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 417-419.

ranking data, because the draft measures do not include the reference to "*the purpose of optimising [Alphabet's] OSE services*".[728]

4.3.3.2.4. The Commission's assessment

(489) The Commission considers that Alphabet must share the Search Data with eligible third-party OSEs on par with Alphabet's own latency for access to the same data for the purpose of optimising its OSE services to the greatest extent that is technically feasible. In addition, the Search Data shall be shared in daily batches and with a daily time stamp.[729] The Commission provides below the reasons for which it specifies this measure.

(490) **First,** Article 6(11) of Regulation (EU) 2022/1925, mandates third parties are provided "*access*" to search data. In order to effectively get access to them, the latency for such access must be determined. Contrary to Alphabet's allegations,[730] Article 6(11) of Regulation (EU) 2022/1925 does provide a legal basis for the determination of the data sharing latency. The term "*access*" implies temporal parameters, which need to be specified in this Decision to ensure this Article to be effective. Contrary to Alphabet's insinuations, the Commission has never required real-time access to the Search Data.[731] Instead it only request Alphabet to share the Search Data with third parties on par with Alphabet's own frequency of access to the same data for the purpose of optimising its OSE services.[732] This Decision further specifies that the latency of data sharing should be as short as technically possible and be no more frequent than 7 days.

(491) **Second**, the Commission considers the principle of parity to be an appropriate framework for determining the parameters of data sharing, including access latency for the reasons specified in section 4.3.1.[733] In addition, the Commission considers that Regulation (EU) 2022/1925 supports the use of parity principle also specifically in relation to the latency of data sharing. In particular, recital 61 of Regulation (EU) 2022/1925 states that the access by Alphabet "*to ranking, query, click and view data constitutes an important barrier to entry and expansion which undermines the contestability of online search engines.*" The "*access*" to data, including the latency with which such data is accessed by third parties, is thus important to remove the data asymmetry between Alphabet and third parties, constituting an important barrier to entry and expansion. From this standpoint, the latency for access to the Search Data should therefore not create further barriers that could make it difficult for third parties to optimise their OSE services. The purpose of Article 6(11) of Regulation (EU) 2022/1925 requires as frictionless access to the Search Data as possible. In this context, data access latency that is on par to Alphabet's own access latency is necessary for third parties to contest Google Search.

(492) Further, the Commission clarifies that the principle of parity means that Alphabet must share the Search Data on par with Alphabet's own latency for access to the same data "*for the purpose of optimising its OSE services"*. Contrary to Alphabet's

728 Alphabet's response to the Revised Measures, Doc ID [...], paragraph 56-57.

729 The text of the measure is repeated here for ease of reading. The binding text is provided in the the Annex to this Decision.

730 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 320-326; Alphabet's submission dated 14 April 2026, Doc ID [...], paragraphs 16-20.

731 The Preliminary Findings refer to the daily latency of data sharing, see Section 5.3.3.3 of Preliminary Findings.

732 Preliminary Findings, Annex, paragraph 15.

733 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 327-347; Alphabet's response to the Revised Measures, Doc ID [...], paragraph 55.

allegations,[734] the principle of parity in relation to data access latency is the same as applied in relation to query, click, view and ranking data. That said, the Commission's view is that the optimisation of OSE services which serves as reference point for the parity principle includes more use cases than the optimisation of search algorithms (see recital (493)) and that parity would in any event support a more frequent latency for data access than the minimum of 7-days as set out in the measures, even considering Alphabet's narrowly scoped reference point of *algorithm* optimisation (see recital (494)).

(493) **Third,** the Commission considers that data access latency should be determined based on parity taking into account different Search Data use cases. The Commission considers that the data access latency is defined within the context of "*optimisation [of OSE] services*" (see recital 61), which encompasses multiple use cases beyond the narrow view that Alphabet takes of optimisation of search algorithms.[735] In particular, it also includes the optimisation of SERP and web index (see recital (18)). Consequently, the principle of parity must take into account the following several distinct reference points:

(a) For the optimisation of SERP, the Commission considers that the parity indicates high frequency of data sharing. [Direct quote describing Alphabet's internal system processes and components].[736] [Description of Alphabet's internal system processes and components].[737]

(b) For the optimisation of index, the Commission also considers that high frequency of data sharing is required. The optimisation based on fresh data is required to identify which new pages and websites the OSE should crawl, to identify trends in users' interests. For instance, [direct quote and data describing Alphabet's internal system processes and timeframes][738] [Direct quote and data describing Alphabet's internal system processes and timeframes][739] [direct quote and data describing Alphabet's internal system processes and timeframes][740] and [direct quote and data describing Alphabet's internal system processes and timeframes].[741]

(c) For the optimisation of search algorithms, the Commission also considers that the parity requires high frequency of data sharing, which can range from real-time to weekly data access, as discussed in the next recital.

(494) **Fourth**, even when considering Alphabet's proposed reference point of algorithm optimisation,[742] the parity indicates that the data access latency should be [description of Alphabet's internal system timeframes]. [Direct quote and timeframe for Alphabet's internal system processes] [743] [Timeframe for Alphabet's internal system processes].[744] What matters for Article 6(11) data sharing is the moment of accessing the data rather than modifying algorithms, which each third-party OSE can

734 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 56-57.
735 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 351-354.
736 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 360(b); see also paragraphs 360-363.
737 Alphabet's reply to RFI 5 of 22 July 2024, Doc ID [...], question 2(a). Alphabet's reply to RFI PO 9 of 5 March 2026, Doc ID [...], question 16.
738 Alphabet's reply to RFI 12 of 13 November 2025, Doc ID [...], Annex Q1.14, page 23.
739 Alphabet's reply to RFI 12 of 13 November 2025, Doc ID [...], Annex Q1.14, page 25.
740 Alphabet's reply to RFI 12 of 13 November 2025, Doc ID [...], Annex Q1.14, page 25.
741 Alphabet's reply to RFI 12 of 13 November 2025, Doc ID [...], Annex Q1.14, page 25.
742 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 348-359.
743 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 358.
744 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 358-359.

carry out on a different timeline, according to their own needs and capacity. Alphabet also agrees with that by stating that "*the relevant question, on the PF's own parity case, is therefore what the frequency is at which Google accesses, for the purpose of optimizing its algorithms, a dataset of the kind it is asked to disclose*" (emphasis added).[745]

(495) [Direct quote and description of Alphabet's internal system processes, components, timeframes and Alphabet's definitions].[746] [Description of Alphabet's internal system processes, components and timeframes].[747] [Direct quote and description of Alphabet's internal system processes, components and timeframes].[748] [Direct quote and description of Alphabet's internal system processes, components and timeframes].[749] [Description of Alphabet's internal system processes, components and timeframes].[750] [Description of Alphabet's internal system processes, components and timeframes].[751] [Description of Alphabet's internal system processes, components and timeframes].[752] [Description of Alphabet's internal system processes, components and timeframes].

Figure 13: [Alphabet's internal document name]

[Image displaying Alphabet's internal system processes]

Source: Alphabet's response to RFI 10, annex Q.14.9, p. 67

(496) Further, the Commission notes that third-party OSEs explain that fresh data is crucial for the optimisation of OSE services. Alphabet misquotes third-party OSEs saying that historical data is sufficient for OSE optimisation.[753] In response to the Commission's question: "*please estimate with which frequency the Art. 6(11) data need to be shared to allow you to optimise your online search engine services"*, eight out of eight market participants replied that the data access latency needs to be near real-time (seven market participants) or at least daily (one market participant).[754]

745 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 354.

746 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 370-373.

747 Alphabet's presentation of 7 May 2026, Doc ID [...], page 13.

748 Alphabet's reply to follow-ups to Tranche 2 Responses to RFIs 10 and 11 of 12 November 2025, Doc ID [...], question 6.

749 Alphabet's reply to RFI 9 of 6 March 2026, Tranche 1, Doc ID [...]question 14.

750 Alphabet's reply to follow-ups to Tranche 2 Responses to RFIs 10 and 11 of 12 November 2025, Doc ID [...], question 6. [Description of Alphabet's internal system processes and components], Alphabet's reply to RFI 12 of 11 May 2026, annex Q1.30, Doc ID [...], page 28. Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 374-374 states that [direct quotes describing Alphabet's internal system processes, components and timeframes]. However, Alphabet's reply to RFI PO 9 of 6 March 2026, Tranche 1, Doc ID [...], Questions 14 and 16 [direct quotes describing Alphabet's internal system processes, components and timeframes].

751 Alphabet's reply to follow-ups to Tranche 2 Responses to RFIs 10 and 11 of 12 November 2025, Doc ID [...], question 6, page 3. See also Alphabet's reply to RFI 10 of 12 November 2025, Annex Q14.9, Doc ID [...], page 50.

752 Alphabet's presentation to the European Commission on Search data & algorithm development dated 2 March 2026, Doc ID [...].

753 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 364-368.

754 [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 11; market participant's reply to RFI of 18 November 2025, Doc ID [...], question 11; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 11; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 11; [market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 11; [market participant's] response to RFI 1 of 18 November 2025, Doc ID [...], question 11; [market participants'] response to RFI of 18 November 2025, Doc ID [...], question 11.

This is to cater for multiple dimension of OSE optimisation, such as ranking optimisation, SERP optimisation and indexing optimisation.[755]

(a) In relation to ranking algorithms, market participants say that outdated data leads to outdated ranking of search results.[756] As put by one market participant: "*our view is that quarterly bulk datasets often reflect outdated search trends and prevent competing search services from identifying evolving user behaviour, daily or hourly search-pattern variation, or the interaction signals required to train relevance and ranking models*" (emphasis added)[757] Four other market participants explain that a shorter time interval (i.e., near real-time latency) for accessing the search data would allow them to analyse temporal trends simultaneously to the events that they relate to, such as sport game results, breaking news events or stock market developments to capture and analyse patterns in queries.[758] They add that this is especially the case for rare or long-tail queries, which are only useful if they are still fresh.[759]

(b) In relation to SERP optimisation, market participants explain that "*a maximum latency of one hour would allow competing search engines to optimi[s]e their SERPs similarly in real time*" (emphasis added).[760] Two market participant state that *"[i]n order to complete a dynamic and competitive search experience, we believe it is essential to have data updated in real time. If this is technically impossible for anonymization reasons, the update frequency should not exceed one hour*."[761]

(c) In relation to indexing, market participants explain that "*[f]resh data is essential for capturing rapid changes in user interests, news events, product launches, and emerging trends. Without timely data, crawling priorities degrade, relevance declines, and the ability to diagnose changes in SERP layout (e.g., introduction of new advanced units) is compromised*" (emphasis added).[762] Another market participant adds that "*[o]n many hot topics (news, random events, sports or game results, ephemeral topics, etc.), it is very important to be able to understand the signals of understanding of the user query and changes in ranking in order to understand, define and implement ranking patterns and crawling strategy*" (emphasis added).

(497) In addition and contrary to Alphabet's suggestions, third parties do not seem to confirm that historical data with a gradual time stamp (e.g., daily) can replace the

---

755 Agreed minutes of a call with [market participant] of 27 October 2023, Doc ID [...], page 4; See also [market participant's] "Response to European Commission Follow Up Questions dated 30 January Regarding Comments on Google's Article 6(11) Compliance" of 12 February 2024, Doc ID [...], question 9; market participant's reply to RFI of 17 February 2026, Doc ID [...], question 12.

756 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 11; [market participant's] reply RFI 2 of 18 November 2025, Doc ID [...], question 11.

757 [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 11.

758 [Market participants'] , "Legal Opinion on Search Data Access under 6(11)" of 4 June 2023, Doc ID [...], paragraph 60. See also [market participants'] reply to RFI 1 of 18 November 2025, Doc IDs [...], [...], question 11(b); market participant's reply to RFI of 18 November 2025, Doc ID [...], 11(a).

759 [Market participants'] "Legal Opinion on Search Data Access under 6(11)" of 4 June 2023 Doc ID [...], paragraph 61.

760 [Market participants'] , "Joint Feedback on Compliance with Article 6(11) DMA (Click-and-Query Data)" of 5 December 2023, Doc ID [...], page 3.

761 [Market participants'] response to RFI of 18 November 2025, Doc IDs [...], [...], question 11(a).

762 [Market participant's] reply to RFI of 18 November 2025, Doc ID [...], question 11. See also [market participant's] presentation of 26 January 2026, Doc ID [...], slide 27.

high frequency of data sharing.[763] They say that gradual time stamp is insufficient and:

(a) "*cannot be used to respond to the trends that are currently happening […] for example, all news and shopping queries require real-time processing*";[764]

(b) "*data reflecting trending and news queries would need to be shared on a near real-time basis – ideally within hours*";[765] and

(c) alongside a daily time stamp "*we would like near real-time data with the oldest query delivered to us within 36 hours before being made*".[766]

(498) **Fifth**, in any event, [Description of Alphabet's internal timeframes], the Commission understands that the latency for data access cannot be more frequent than [1-7] days, for technical reasons, and some additional days to apply the anonymisation measures and share data. [Description of Alphabet's internal timeframes].[767] [Description of Alphabet's internal timeframes][768]

(499) Subject to the provided information being accurate and correct, the Commission accepts that there is a minimum of [1-7] days required for Alphabet to process the data, [description of Alphabet's internal system timeframes].[769] In addition, the Commission recognises that some additional specific steps will be needed. The Commission sets a lower bound of [1-7] days for these additional steps. The Commission therefore considers that the latency for data access should not be less than 7 days. The measures further specify that, based on the final data scope and anonymisation measures, Alphabet must communicate the final latency of Search Data within the timeframe specified in section 4.6, ensuring that the proposed latency is the lowest technically feasible. Additionally, Alphabet must provide a detailed technical description and justification explaining why the steps it envisages are all strictly necessary and why the proposed latency of each step is reduced to the strict minimum, including verifiable information that can be tested by interested third parties. Alphabet must subsequently notify the beneficiaries of the final latency for sharing the Search Dataset.

(500) **Sixth**, the at least 7-day-latency for data access also addresses Alphabet's concerns regarding the proportionality of high-frequency data sharing and alleged harm to Google Search, Google Search's users and third-party websites.[770] Alphabet raises that the high-frequency disclosure exacerbates the risk that data recipients would copy Google's and third parties web content, reveal the information on their commercial performance, and increase the risk of reidentification, which taken

763 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs, 366, 380-382.

764 Agreed minutes of meeting with [market participant] , Doc ID [...], page 4, which contradicts Alphabet's quotes in its response to the Preliminary Findings, Doc ID [...], paragraph 366(a) and 382(a)

765 Market participant's reply to RFI 1, Doc ID [...], question 11, which contradicts Alphabet's quote in its response to the Preliminary Findings, Doc ID [...], paragraph 366(b).

766 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 11, which contradicts Alphabet's quote in its reply to the Preliminary Findings, Doc ID [...], paragraph 366(d and e) and 382(b). Similarly also [market participants'] reply to RFI of 18 November 2025, Doc IDs [...], [...], question 11. Alphabet's last quote (Minutes of meeting with [market participant], Doc ID [...]) is besides the point, as it relates to syndication rather than the required latency for OSE optimisation

767 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 416-420.

768 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 417; Alphabet's response to RFI PO 12 of 11 May 2026, Doc ID [...], questions 7 and 8.

769 Alphabet's reply to the RFI PO 12 of 11 May 2026, Doc ID [...], question 7.

770 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 388-415. See also Alphabet's submission dated 14 April 2026, Doc ID [...], paragraphs 20-32.

together make the high-frequency data sharing disproportionate.[771] The Commission assesses these risks as low to begin with. Regarding the concern that third parties might replicate Google's search results, the Search Data provides only a partial snapshot of the data required to operate an OSE service, necessitating substantial additional work by third-party OSEs (see recital (198)). Similarly, the risk of third parties replicating the inventory of third-party websites is mitigated, as each query contains only a limited selection of products, making full replication impractical (see recitals (347) and (410)). Additionally, there is no risk of exposing advertisers' bid strategies or commercial and financial performance, as the Search Data excludes ad URLs and related user interaction data (see section 4.4.4.1). Likewise, the risk of third parties appropriating content from third-party websites is minimal, since the Search Data does not contain website content but only publicly available URLs (see recital (346)). Furthermore, the anonymisation process is robust, eliminating any risk of re-identification (see section 4.4.4.1). In any event, the Commission considers that the 7-day minimum latency for data access effectively addresses Alphabet's concerns by introducing a delay into the accessibility of the data. This lag ensures that data recipients are unable to use the information immediately, thereby reducing significantly any potential for automatism and rapid response. By staggering the release of data, the measures mitigate the risk of immediate replication or exploitation.

(501) **Seventh**, the measures specify that Alphabet must share the Search Data in daily batches (justified by anonymisation requirements (see section 4.4.4.1). This means that the Search Data generated on day 1 must be shared on day 8 (assuming the latency of 7 days) and the Search Data collected on day 2 must be shared on day 9 (assuming the same latency). The daily batches also mean that the Search Data includes a daily time stamp (e.g., the fact that a given data comes from day 1 or day 2). While currently the Google Search Data does not come in daily batches or includes a daily time stamp, Alphabet does not contest these measures. For example, Alphabet states that the *"[t]raining of algorithms to detect and adjust to new developments and events can be achieved through an appropriate time resolution, i.e., the granularity of the time stamp"* [772] The Commission also considers that the daily batches and time stamp are required for the following reasons:

(a) ***In the first place***, the time stamp data is part of *"query data"* referred to in Article 6(11) of Regulation (EU) 2022/1925. As explained in recitals (216)-(221), the concept of *"query data"* is broader than the query text and includes all data used to complement search queries and identify matching results, such as the query's timing.

(b) ***In the second place***, the parity principle requires Alphabet to share the Search Data in batches and with time stamp data at the same level of granularity as Alphabet itself relies on. [Description of Alphabet's internal system processes, components, and timeframes].[773] [Description of Alphabet's internal system processes, components, and timeframes].[774] These are useful reference points,

---

771 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 388-415. See also Alphabet's submission dated 14 April 2026, Doc ID [...], paragraphs 20-32.

772 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 376-381.

773 Alphabet's reply to RFI 6 of 13 July 2025, Doc ID [...] question 5.

774 [Description of Alphabet's internal system processes and components]. See Alphabet's response to RFI PO 9, Tranche 2, Annex Q13, Doc ID [...], raw no. 16. See also Alphabet's response to RFI 10 of 12 November 2025, Annex Q5, Doc ID [...], page 4.

even though the measures ultimately specify the daily graduality because of anonymisation needs (see section 4.4.4.1).

(c) In addition, the Commission notes that market participants confirm that frequent batches and query time stamps are needed for the optimisation of their OSE services. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 4.7 on a scale from 1-5, meaning that such data is on average "*essential*" for market participants.[775] They also refer to time stamps of great granularity, such as "*exact time [of query], accuracy to minute*",[776] "*hour granularity*"[777] or "*day*"[778] granularity. One market participants explains that "*we need to know what state the internet was in at the time the query was made: which documents didn't exist yet (to exclude these from our model training), what news articles were 'fresh' (a feature) and whether the query was 'newsy'/'buzzy'/'trending'.*"[779]

(502) Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, the Search Data should be shared with a latency of at least 7 days, come in daily batches and with a daily time stamp.

4.3.3.3. Method of sharing

4.3.3.3.1. Introduction

(503) Data can be shared in several different technical ways. For example, it might be provided as large files that third-party OSEs can download on a recurrent basis, or it might be made available through an online connection between computers, the so-called Application Programming Interfaces ("**APIs**").

(504) Currently, the method of sharing of Google Search Data is as follows:

(a) The dataset can be downloaded by third parties from Google Cloud in JSON open standard format;[780] and

(b) Third parties can either download the full dataset covering all EEA countries to which they direct services, or sections of the dataset by country.[781]

4.3.3.3.2. Measures

(505) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must use the method of sharing that it uses itself internally for sharing the Search Data with eligible third-party OSEs to the greatest extent that is technically feasible, avoiding unnecessary cost or operational friction, and in any case the method of

---

775 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to Annex 1 of the Commission's RFI PO 1 dated 28 January 2026, Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], Doc ID [...], and Doc ID [...]. See also [market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2 and [Market participants'] Submission dated 5 December 2023, Doc ID [...], page 1.

776 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2.

777 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2.

778 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 5.

779 [Market participant's] reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID [...], page 2.

780 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 2; Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 5; Alphabet's reply to RFI 4 of 6 May 2024, Doc ID [...], question 25.

781 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], question 5.

sharing needs to enable effective sharing of Search Data. Alphabet should provide technical support to third-party OSEs accessing the Search Data.

4.3.3.3.3. The gatekeeper's view

(506) In response to the Preliminary Findings, Alphabet argues that the sharing of Search Data via an API would require Alphabet to build new infrastructure, which is not practically possible.[782] In addition, Alphabet combines its arguments on the frequency of data sharing with the method of sharing. It states that the close to real-time data sharing via an API would allow recipients to copy Google's results, [783] would distort the search syndication market,[784] and would pose significant security risks, including the potential for compromised credentials, vulnerabilities, or insider threats, which could create a pathway back into Google's systems (on these arguments see section 4.3.3.2). [785]

(507) In response to the revised specification measures, Alphabet approves the removal of API-based access and requests a clarification that the dataset should be made available via a downloading process.[786]

4.3.3.3.4. The Commission's assessment

(508) As set out in section 4.3.3.3.2, the Commission specifies that Alphabet must share the Search Data via a method equivalent to Alphabet's own method of accessing such data, taking into account what is technically possible and cost-efficient.[787] The Commission clarifies that while the measures do not include a reference to an API, this does not imply that the API is not required or endorse Alphabet's proposal to share the Search Data with a file for download.[788] Below, the Commission gives reasons why it considers necessary to specify this measure.

(509) **First,** Article 6(11) of Regulation (EU) 2022/1925 explicitly requires Alphabet to "*provide to any third-party undertaking providing online search engines, at its request, with access to [search data]*" (emphasis added). It follows that the data sharing method should enable third parties to access the Search Data at their request, which implies some flexibility. As explained in recital (513), the access to the data through an API or a similar method allows for more flexibility and better capability than a downloading,[789] and therefore fits the prescription of Article 6(11) of Regulation (EU) 2022/1925.

(510) **Second**, sharing data via an API or a similar method instead of a downloading is supported by recital 61 of Regulation (EU) 2022/1925. Recital 61 states that the access by gatekeepers, such as Alphabet, "*to ranking, query, click and view data constitutes an important barrier to entry and expansion which undermines the contestability of online search engines.*" From that standpoint, the method of access to the Search Data should not create further barriers that could make it difficult for third parties to optimise their OSE services. The purpose of Article 6(11) of Regulation (EU) 2022/1925 requires as frictionless access to the Search Data as

782 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 525 and 548.
783 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 48.
784 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 501.
785 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 586.
786 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 97-101.
787 The text of the measure is repeated here for ease of reading. The binding text is provided in the the Annex to this Decision.
788 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 97-101.
789 Contrary Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 97-101 and in particular paragraph 100.

technically possible. In that sense, an API or a similar method is a more suitable data sharing method than a downloading, since it provides for constant, continuous and flexible access to the Search Data, supporting third parties in the optimisation of their OSE services.

(511) **Third,** the principle of FRAND requires that the method of data sharing should correspond to industry standards, which suggests data sharing through APIs or similar methods. APIs remain the most popular method for sharing large datasets due to their flexibility, scalability, and ease of use. According to [third party], 82% of companies use APIs to share data.[790] APIs are appreciated because of the opportunities for integration and interoperability with companies' own systems, flexibility of accessing various data points, ability to handle large datasets, data analytics and security.[791]

(512) **Fourth**, having an API or a similar method as Alphabet's data sharing method would meet the principle of parity. [Description of Alphabet's internal system processes and components].[792] [Description of Alphabet's internal system processes and components].[793] As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. [Description of Alphabet's internal system processes and components],[794] [description of Alphabet's internal system processes and components].

Figure 14: [Alphabet's internal document name]

[Image displaying Alphabet's internal system processes and components]

Source: Alphabet's response to RFI 10, Annex Q1.19, p. 45

(513) **Fifth**, Alphabet shares even Google Trend data, a publicly available sample of Google Search data, via an API.[795] Alphabet notes this dataset is *"much less detailed and granular, […] compared to the search dataset"* (emphasis added).[796] However, this indicates that the Search Data - which is a larger and more complex dataset - all the more need to be shared via an API, which is considered as a sharing tool particularly fit for vast datasets.

(514) **Sixth,** third parties confirm that the data access through an API is required by them to optimise their OSE services. Market participants expressed a strong preference for an API as the favoured method of sharing over downloading.[797] They explain that:

---

790 https://www.postman.com/state-of-api/2025/#introduction, Doc ID [...], last accessed on 13 April 2026.

791 https://www.dataversity.net/articles/12-benefits-of-data-sharing-via-apis/, Doc ID [...], last accessed on 13 April 2026.

792 In the US vs. Google remedy judgment, the court noted that "*Google trains Navboost on 13 months of user data."* US vs. Google, Memorandum opinion of 2 September 2025, Doc ID [...], Page 157; Alphabet's reply to question 6 of RFI 10 of 12 November 2025, Tranche 2, Doc ID [...], paragraph 29.

793 Alphabet's reply to follow-ups to Tranche 2 Responses to RFIs 10 and 11 of 12 November 2025, Doc ID [...], question 6. Alphabet's reply to RFI 12 of 13 November 2025, Annex Q1.19, Doc ID [...], page 7.

794 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 97-99.

795 Alphabet's reply to RFI 4 of 15 May 2024, Tranche 3, Doc ID [...], question 20.

796 Alphabet's reply to RFI 4 of 15 May 2024, Tranche 3, Doc ID [...], question 20.

797 [Market participant's] submission of 15 June 2023, Doc ID [...], page 1; [market participant's] submission of 16 January 2024, Doc ID [...]; [market participant's] reply to RFI of 18 November 2023, Doc ID [...], question 11.

(a) An API is their preferred method of accessing the data, as it would allow them to first organise and process data before they can use it to power indexing and ranking algorithms;[798]

(b) A sharing via an API is the best method for the near real-time data sharing. If the Search Data is shared through an API, this would enable third parties to optimise their search similarly in real-time;[799]

(c) APIs allow for a flexible data access. With the API, third parties would have the option to access and use only new data, rather than have to access the complete dataset every time;[800] and

(d) APIs allow for tailoring the terms of access to own needs and the integration of Search Data with third parties' search technologies and data analytics tools. APIs give interoperability and tooling options. For example, APIs provide a programmatic interface for accessing data, allowing developers to integrate data into their applications and services easily.[801]

(515) Therefore, to ensure that third-party OSE "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, the Search Data should be shared via a method equivalent to [Alphabet's internal system component] or equally performant method of sharing. The API or similar sharing method must also enable third parties to access only new data, rather than the complete updated dataset every time they use the API to enable a truly flexible data access.[802]

(516) **Seventh**, Alphabet considered the API to be unnecessary.[803] However, that conclusion was based on Alphabet's decision to provide the dataset every three months.[804] As is set out in section 4.3.3.2, the Commission's measures specify more frequent data sharing, which requires an API or a similar method of sharing. Alphabet also deemed the API an unsuitable method for data sharing, as the dataset, with around 20TB of data, would be too large to access via the API.[805] However, Alphabet did not further substantiate why the size of the dataset would be a technical barrier to adopt the API as the method of sharing. In that context, a third party noted that Alphabet already licenses its search results, including ad data, via real-time APIs to some competitors.[806] Further, Alphabet stated that it would need to build a new API, which is not practically possible.[807] However, Alphabet did not substantiate this claim.[808]

(517) **Eight,** in any event, if an equivalent method of sharing to the one Alphabet utilises internally for sharing the Search Data with third parties is not technically feasible,

---

798 [Market participants'], "Joint Feedback on Compliance with Article 6(11), DMA (Click-and-Query Data)" of 5 December 2023, Doc ID [...], page 3.

799 [Market participants'] "Joint Feedback on Compliance with Article 6(11), DMA (Click-and-Query Data)" of 5 December 2023, Doc ID [...], page 3.

800 [Market participant's] "Comments on Google's Digital Markets Act Article 6(11) Compliance Proposal" of 17 January 2024, Doc ID [...], page 5.

801 https://www.dataversity.net/articles/12-benefits-of-data-sharing-via-apis/, Doc ID [...], last accessed on 13 April 2026.

802 See the following replies to the public consultation responses: [third party], Doc ID [...]; [third party], Doc ID [...].

803 Alphabet's reply to RFI 4 of 6 May 2024, Doc ID [...], question 25.

804 Alphabet's reply to RFI 4 of 6 May 2024, Doc ID [...]2, question 25.

805 Alphabet's reply to RFI 4 of 6 May 2024, Doc ID [...]2, question 25.

806 [Market participant's] submission of 12 September 2025, Doc ID [...], page 5.

807 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 525(b) and 548.

808 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 525(b) and 548. Paragraph 525(b) reads: [Direct quote describing Alphabet's internal processes].

then Alphabet should employ the closest possible method of sharing that achieves the same objective. Whilst doing so, Alphabet must avoid unnecessary cost or operational friction for data recipients, ensuring that the approach adopted is practical and efficient. Nevertheless, in selecting an alternative method, the primary consideration should be the ability to facilitate effective sharing of Search Data, thereby ensuring that the desired outcomes are met.

(518) **Ninth,** for the Search Data sharing to be effective and workable in practice, Alphabet must offer adequate technical assistance and support to access the Search Data. Article 6(11) of Regulation (EU) 2022/1925 is results-oriented and third parties need to be in a position to effectively access the Search Data. It is also in line with the principle of parity that Alphabet follows its usual practices in relation to sharing large datasets, including any testing and troubleshooting. The Commission's own attempts to access a sample of search data have occurred to be difficult to realise in practice given numerous technical issues encountered (e.g., problems with logging in, limited data access, technical glitches). Against that background, Alphabet must offer necessary technical support to third parties to ensure that they have an effective access to the Search Data.

4.3.3.4. Duration

4.3.3.4.1. Introduction

(519) As laid down in recital 61 of Regulation (EU) 2022/1925, the objective of that Regulation is to enable third-party OSEs to "*contest"* Google Search.

(520) Alphabet intends to share the Google Search Data for three years with each third party who concludes a licence under Alphabet's Search Dataset Licensing Program.[809] Alphabet considers that afterwards any OSE recipient should have received sufficient data to train their algorithms and overcome any conceivable data disadvantage.[810] Alphabet stresses that a perpetual data disclosure obligation would be disproportionate.[811]

4.3.3.4.2. Measures

(521) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must share the Search Data with eligible third-party OSEs for the period of their choice and up to five years starting from the moment when the Search Data becomes effectively accessible to that specific third party.

(522) Notwithstanding, the Commission reserves the right to reassess and potentially revise the specification of this duration if it determines that the maximum five-year period of Search Data sharing is not sufficient to achieve the objectives set out in Article 6(11) of Regulation (EU) 2022/1925, in accordance with Article 8(9) thereof.

(523) This is without prejudice to Alphabet being obliged to continue offering the Search Data to eligible third-party OSEs for the entire duration of Google Search's designation as a CPS.

---

809 Alphabet's Google European Search Licensing Program, Doc ID [...], page 2.

810 Alphabet's reply to RFI 1 of 23 November 2023, Doc ID [...], questions 2 and 19, and Alphabet's reply to RFI 2 of 22 December 2023, Doc ID [...], question 6.

811 Reply to RFI 1 of 23 November 2023, Doc ID [...], question 19. Alphabet makes the search dataset available for download via Google Cloud in the JSON open standard format, see reply to RFI 4 of 15 May, 3 Tranche, Doc ID [...], question 25.

4.3.3.4.3. The gatekeeper's view

(524) In response to the Preliminary Findings, Alphabet argues that the minimal duration of five years specified in the Preliminary Findings is disproportionate due to (i) not stipulating a maximum period, hence envisaging an indefinite obligation,[812] (ii) being incompliant with the FRAND licensing, [813] and (iii) market participants needing only zero to five years to optimise their OSE services. [814] Alphabet does not propose a concrete duration in response to the Preliminary Findings, but it confirms that a reasonable period during which third parties should rely on the dataset, based on the evidence of Preliminary Findings, is up to five years.[815]

(525) In the observations on the Revised Measures, Alphabet argues that (i) the five-year duration is not necessary to achieve the objective of integrating search data and contest Google Search,[816] (ii) evidence of third parties does not support a duration over three years,[817] (iii) the Commission must have proper regard to the impact on Alphabet's intellectual property.[818] Alphabet further proposes a revision of license duration to maximum three years.[819]

4.3.3.4.4. The Commission's assessment

(526) As set out in section 4.3.3.4.2, the Commission specifies that Alphabet must share the Search Data with any third-party undertakings providing OSEs for the period of their choice and up to five years.[820] For the avoidance of doubt, the Decision does not require Alphabet to conclude data sharing agreements with individual third parties for a period longer than five years.[821] Below, the Commission provides reasons for which it specifies this measure.

(527) **First**, Article 6(11) of Regulation (EU) 2022/1925 does not specify a time limit for Alphabet's obligation to share the Search Data. However, the purpose of Article 6(11) of Regulation (EU) 2022/1925, as stated in recital 61 of that Regulation, is to enable third-party OSEs to "*optimise their services and contest the relevant core platform services*." It follows from this objective that third parties must be provided sufficient time to integrate search data, enhance their existing capabilities and become capable of contesting Google Search. At the same time, Article 6(11) of Regulation (EU) 2022/1925 does not lay down a perpetual data sharing obligation and third parties should access the Search Data as a transitional measure to overcome barriers to entry and expansion, develop independent OSEs and become capable of contesting Google Search.[822]

(528) **Second,** Article 6(11) of Regulation (EU) 2022/1925 requires that the Search Data are shared on FRAND terms. This means that the duration of data sharing should be fair and reasonable, given the objective of Article 6(11) of Regulation (EU) 2022/1925, namely allowing third parties to optimise their OSE services and

812 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 536-538.
813 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 539-540.
814 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 541-542.
815 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 538 and 545.
816 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 90 and 91.
817 Alphabet's response to the Revised Measures, Doc ID [...], paragraph 95.
818 Alphabet's response to the Revised Measures, Doc ID [...], paragraph 93.
819 Alphabet's response to the Revised Measures, Doc ID [...], Annex, page 6.
820 The text of the measure is repeated here for ease of reading. The binding text is provided in the the Annex to this Decision.
821 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 536-546.
822 In line with Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 537-539.

avoiding Alphabet to support rivals indefinitely.[823] The Commission considers that the five-year limit regarding the duration of data sharing addresses Alphabet's concerns about long-term copying of its technologies,[824] as it provides an incentive for third-party OSEs to work on their independent OSE technologies given that data sharing contracts will eventually end.

(529) **Third**, to achieve the objectives specified in Article 6(11) of Regulation (EU) 2022/1925, third-party OSEs must have access to the Search Data for a period of their choice and up to five years starting from the moment when the Search Data becomes effectively accessible to them. The optimisation of OSE services is a long-term process. Third parties estimate that just the data integration process would likely take some time.[825] This integration process is also just a beginning. It paves the way to the long-term continuous work to optimise OSE services based on newly available search data, which would take [zero – five] years.[826] One market participant explains that process step by step:

(a) "Data Acquisition and Index Coverage: Integrate new data feeds and achieve comprehensive.

(b) *Development of Ranking Algorithms: Develop and refine ranking algorithms to optimise result quality.*

(c) *User Feedback and Continuous Optimisation: Collect sufficient user adoption and interaction signals to feed back into ranking and UI improvements."*[827]

(530) Therefore, to ensure that third-party OSEs "*can optimise their services and contest the relevant core platform services*", as set out in recital 61, the Search Data should be shared by Alphabet for a period of their choice and up to five years.

(531) Alphabet argues that third-party OSEs do not require five years to optimise their OSE services, and three years should be sufficient.[828] The Commission does not agree with these conclusions. Alphabet distorts the evidence referring to a timeline for single training cycle, while multiple cycles are required for OSE optimisation.[829] For example, Alphabet states that one market participant requires one and a half to three years to complete a training cycle, while this stakeholder actually states that "*we would need multiple full seasonal cycles to accurately model and train […] 3-year data sharing duration under Alphabet's program is not sufficient to optimise […] 5–7+ years of continuous, rolling access is the realistic minimum*".[830] Contrary to Alphabet's claims,[831] the majority of third-party OSEs submit that they need five years or longer to optimise their OSE services, with many of them arguing for access to Search Data as long as Google Search maintains its position as a core platform

---

823 In line with Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 540.

824 Alphabet's response to Preliminary Findings, Doc ID [...], paragraphs 541-546. Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 93-95.

825 [Market participant's] response to RFI PO 1 of 28 January 2026, Doc ID [...], question 6.

826 [Market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], page 11.

827 [Market participant's] reply to RFI PO 1 of 28 January 2026, Doc ID [...], page 11.

828 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 90-92, 95.

829 Alphabet's response to the Revised Measures, Doc ID [...], paragraph 92.

830 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 13. [Market participant] also only refers to the "*initial*" training cycle, see [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 13. Similarly, the market participant in reply to RFI 1 of 18 November 2025, Doc ID [...], refers to "*multiple*" training cycles and that the "*search infrastructure optimization is an ongoing process rather than a discrete project with a fixed endpoint*."

831 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 541-545.

service.[832] Third-party OSEs are also clear that the three-year duration of data sharing is insufficient. For instance, one market participant noted that *"[s]earch engine optimisation is a complex process, and three years would not be sufficient to complete the full optimisation cycle."*[833] As put by another market participant: "[*t]he underlying data asymmetry is structural and ongoing, and search-engine optimisation is continuous. If access to data were discontinued after three years, the asymmetry would immediately re-emerge*."[834] Moreover, submissions to the public consultation considered the increase in duration *"a substantial improvement over the current situation",*[835] whereas some endorsed that five years should be *"a minimum period and not a cap."*[836] Third parties therefore require a sufficiently long access to the Search Data to at least establish an independent robust data flywheel and be in position to contest Google Search.

(532) **Fourth**, while the measures specify that the duration of Search Data sharing should be up to five years, the Commission reserves the right to reassess and potentially revise the specification of this duration if it determines that the maximum five-year period of Search Data sharing is not sufficient to achieve the objectives set out in Article 6(11) of Regulation (EU) 2022/1925. It is essential to consider that Google Search has had more than 85% of market share in most EU Member States throughout for more than a decade and managed to optimise its search technologies on vast user datasets year by year.[837] Google Search enjoys this data advantage to this day. For example, In the US vs. Google remedy judgment, the court noted that "*Google trains Navboost on 13 months of user data, which is the equivalent of over 17 years of data received by Bing*".[838] Having considered various expert testimonies on the required remedy duration, including those assessing the impact of data sharing on Alphabet's intellectual property,[839] the court concluded that *"Google's proposed term of three years is simply too short"*[840] and that the data sharing remedy duration should be *"a five-year term, plus an additional one year to put the infrastructure and processes in place to implement the remedies".* [841]

(533) As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself has had time to access to the Search Data for the purpose of optimising its OSE services for a long time, and considering that this data is required for OSE optimisation for a substantial period of time, Alphabet's a reasonable duration of licence agreements to the Search Data is required for third parties to overcome barriers to entry and expansion and contest Google Search, as identified in recital 61 of the Regulation. To that end, the Commission reserves the right to

---

832 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 13; [Market participant's] reply to RFI 1 of 18 November 2025, Tranche 2, Doc ID [...], question 13(1); [Market participants'] , Legal Opinion on Search Data Access under 6(11) of 4 June 2023, Doc ID [...], paragraphs 64-65; [Market participant's] reply to RFI 2 of 18 November 2025, Doc ID [...], question 13. See also the replies to the public consultation responses from [third party], Doc ID [...]and [third party], Doc ID [...].

833 [Market participant's] reply to RFI 1 of 18 November 2025, Tranche 2, Doc ID [...], question 13(1);

834 [Market participant's] reply to RFI 1 of 18 November 2025, Doc ID [...], question 13.

835 Response to the public consultation from [third party], Doc ID [...].

836 Response to the public consultation from [third party], Doc ID [...].

837 Commission's Decision in AT.39740, *Google Shopping*, C(2017) 4444, paragraph 271 et seq.

838 US vs. Google, Memorandum opinion of 2 September 2025, Doc ID [...], page 157.

839 Alphabet's response to the Revised Measures, Doc ID [...], paragraphs 93-96.

840 US vs. Google, Memorandum opinion of 2 September 2025, Doc ID [...], page 224.

841 US vs. Google, Memorandum opinion of 2 September 2025, Doc ID [...], page 225.

reassess and potentially revise the specification of duration of Search Data Sharing beyond five years.

(534) **Fifth**, notwithstanding the duration of third parties' individual access to the Search Data under this Decision, Alphabet should in any case offer Search Data under Article 6(11) of Regulation (EU) 2022/1925 for as long as Google Search is designated as a CPS. For example, if a given OSE reaches out to Alphabet six years after the adoption of this Decision and Google Search is still a designated CPS, Alphabet should offer concluding a Search Data sharing agreement with this stakeholder for the period of their choice and up to five years.

4.3.3.5. Search session data

4.3.3.5.1. Introduction

(535) Users sometimes enter several queries to find a response to their questions. They enter a query, review search results, and modify their query again with slightly different words. If this happens close together in time, OSEs treat the consecutive queries and the associated search results and user interaction with these results as a single "search session". Search sessions help OSEs understand the query intent and adapt the search results accordingly.

(536) The Google Search Data does not link different queries that a user issues and the associated other search data in a session because of anonymisation concerns.[842]

(537) In the following section, the Commission provides its assessment in relation to search session data. While the Commission considers that search session data falls under "*ranking, query, click and view data*", it limits the sharing of session data to a so-called mini-sessions whose maximum length is three queries. The measure requiring the sharing of mini-sessions is set out in the below section 4.4.4.1.1 at recitals (606) and (607).

4.3.3.5.2. The gatekeeper's views

(538) Beyond the general claim that the measures expropriate the value from Alphabet organising, processing and transforming row user data into [description of Alphabet's internal system processes and components] for use by its search algorithms,[843] Alphabet's main claims against the sharing of session data concern the risk of re-identification and are therefore addressed in Section 4.4 of this Decision.

4.3.3.5.3. The Commission's assessment

(539) The Commission considers that, subject to anonymisation requirements, Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share search sessions data because it qualifies for "*ranking, query, click and view data*" in the meaning of this provision. This is for the following reasons.

(540) **First**, the requirement to share search sessions data does not require Alphabet to provide any additional data which does not fall under ranking, query click or view data categories. The only added element of search sessions is that the ranking, query, click and view data is organised in a way that allows to identify the consecutive user actions, such as queries and user interactions from the same user within a certain time window. This is data already shared, what Alphabet is required to add is simply a session identifier to the dataset's structure. No specific new data type is required.

842 Alphabet's reply to RFI 8 of 22 July 2024, Doc ID […], Question 3, paragraph 9.

843 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 32. This claim is addressed in section 4.3.1 of this Decision.

Therefore, session data is within the scope of Article 6(11) of Regulation (EU) 2022/1925.

(541) **Second**, recital 61 of Regulation (EU) 2022/1925 describes search data broadly. It frames click, query, view and ranking data as the data intended to enable third-party OSEs understand the entire chain of user interactions with the gatekeeping OSEs. Recital 61 states that third-party OSEs should have access to gatekeepers' "*datasets containing information about what users searched for, and how they interacted with, the results with which they were provided*". Session data is key to fully interpret how users interact with results. Article 6(11) of the Regulation should therefore be interpreted to require the sharing of ranking, query, click and view data in a way that allows maximising the value of such data, including the grouping of the data to allow the identification of search sessions.

(542) **Third**, the parity principle requires Alphabet to share search sessions, grouping Search data in [direct quotes and description of Alphabet's internal system processes, components, and timeframes].[844] [Direct quotes and description of Alphabet's internal system processes, components, and timeframes],[845] [direct quotes and description of Alphabet's internal system processes, components, and timeframes].[846] [Direct quotes and description of Alphabet's internal system processes, components, and timeframes].[847] [Direct quotes and description of Alphabet's internal system processes, components, and timeframes]. As explained in section 4.3.1, the Commission considers that the relevant standard for data sharing pursuant to Article 6(11) of Regulation (EU) 2022/1925 is parity. As Alphabet itself collects such data for the purpose of optimising its OSE services, the data should be shared as part of the Search Dataset.

(543) **Fourth,** the data is important input for the optimisation of OSE services. ***In the first place***, Alphabet's internal documents demonstrate the importance of search session data to provide relevant search results to users. For example, Google's internal email stresses that search session data provide Google Search with a competitive advantage: *"Google concedes that scale gives Google a 'competitive advantage' and that scale is the 'magic' behind Google's success. [..] "[M]ost of the knowledge that powers Google, that makes it magical, originates in the minds of users. Users are the founts of knowledge--not us.") [..] "After a few hundred billion rounds we start lookin' pretty smart! This isn't the only way we learn, but the most effective." [..] "<u>But *sessions logs* are our unique competitive advantage</u>".*[848]

(544) ***In the second place***, third parties confirm that search session data is an important input for OSE optimisation. The average rating by market participants who replied to the Commission's RFI on the importance of this data for OSE optimisation was 3.3, meaning that market participants consider such data between "*moderately important*" to "*very important*".[849] One market participant explained that *"[s]essions and reformulation data are an essential part for optimising the relevance of a search*

---

844 Alphabet's reply to questions 9, 12, 16 and 37 of RFI 2 of 30 January 2026, Tranche 2, Doc ID […].

845 Alphabet's reply to question 6 of EC follow-up question of 7 January 2026, Doc ID […].

846 Alphabet's reply to question 12 of RFI PO 9, Doc ID […]. [Description of Alphabet's internal system processes].

847 Alphabet's reply to question 6 of EC follow-up question of 7 January 2026, Doc ID […].

848 Alphabet's internal document quoted in U.S. and Plaintiff States v. Google LLC vs [2020], Case No. 1:20-cv-03010 (D.D.C.), paragraph 166.

849 Where 1= not important, 2= low importance, 3= moderately important, 4= very important, 5= essential. See the replies of third parties to RFI PO 1 dated 28 January 2026, Annex 1, Doc ID […]; reply of a market participant to RFI of 17 February 2026, Annex 1, Doc ID […].

engine's results".[850] It adds that without search session data it has *"no information about whether the search was satisfactory or not and whether the user reformulated his query to hopefully get more relevant results".*[851] A second market participant added that search session data *"[h]elps understand intent evolution (reformulations) and interpret sequences (including click-backs)".*[852] A third market participant explained that *"[k]nowing how users rephrase their queries and how they behave within a single session helps us understand how users interact with the search system".*[853]

(545) **Fifth,** as explained in section 4.4.4.1.2.1.5, the Commission's anonymisation approach does not allow for the releasing of full sessions given the high privacy risk that this would entail. Instead, sharing should be limited to so-called mini-sessions whose maximum length is three queries.

(546) **Sixth**, as explained in Section 4.3.1.3, providing session data will not expropriate Alphabet's intellectual property and innovation, nor will they limit innovation. Any reliance of the measures on Alphabet's effort or innovation do not go beyond what was intended for by the legislator in drafting Regulation (EU) 2022/1925.

4.4. Measures relating to anonymisation

4.4.1. Legal framework

(547) Article 6(11) of Regulation (EU) 2022/1925 read in the light of recital 61 of that Regulation explains that a gatekeeper should ensure the protection of the personal data of end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data and that this should be done without substantially degrading the quality or usefulness of the data. That recital also provides that "[t]*he relevant data is anonymised if personal data is irreversibly altered in such a way that information does not relate to an identified or identifiable natural person or where personal data is rendered anonymous in such a manner that the data subject is not or is no longer identifiable*."

(548) Article 4(1) of Regulation (EU) 2016/679 defines personal data as any information relating to an identified or identifiable natural person. Recital 26 of Regulation (EU) 2016/679 explains that to determine whether a natural person is identifiable, all the means reasonably likely to be used must be taken into account, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. All objective factors must be taken into account as well, such as the costs of and the amount of time required for identification, the available technology at the time of the processing and technological developments.

(549) In so far as recital 26 refers to the means likely reasonably to be used by both the controller and by "*any other person*", the CJEU case law states that it is not required that all the information enabling the identification of the data subject must be in the hands of one person to qualify as personal data.[854] At the same time, data would not

850 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

851 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

852 [Market participant]'s reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID […], page 7.

853 [Market participant]'s reply to RFI PO 1 of 28 January 2026, Annex 1, Doc ID […], page 6. See also [market participant]'s presentation of 26 January 2026, Doc ID […], slides 8-9.

854 Judgment of the Court of Justice of 19 October 2016, *Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, paragraphs 43, See also Judgment of the Court of Justice of 9 November 2023, *Gesamtverband Autoteile-Handel eV v Scania CV AB*, C-319/22, ECLI:EU:C:2023:837, paragraph 45; Judgment of the Court of Justice of 7 March 2024, *IAB Europe v Gegevensbeschermingsautoriteit*, C-604/22, ECLI:EU:C:2024:214, paragraph 40.

qualify as personal data where the identification of the data subject is prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and manpower, so that the risk of identification appears in reality to be insignificant.[855]

(550) According to further CJEU case law, "*pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable*"[856], with the result that the data is not personal for them.[857] However, that presupposes, firstly, that the recipient of the pseudonymised data "*is not in a position to lift [the technical and organisational] measures [implementing the pseudonymisation]*" "*during any processing of the [pseudonymised data] which is carried out under its control*".[858] Secondly, it also presupposes that "*those measures must in fact be as such as to prevent* [the recipient] *from attributing those* [pseudonymised data] *to the data subject including by recourse to other means of identification such as cross-checking with other factors, in such a way that, for the* [the recipient], *the person concerned is not or no longer identifiable*".[859]

(551) In addition, Article 6(11) of Regulation (EU) 2022/1925 read in the light of recital 61 of that Regulation provides that the anonymisation requirement applies to the personal data of the end user generating the data and not to the personal data of other individuals that might be identifiable via ranking, query, click and view data (e.g., personal data mentioned in query and ranking data). Regulation (EU) 2016/679 remains applicable to the sharing of or granting access to personal data of other individuals that are identifiable via ranking, query, click and view data shared by gatekeepers pursuant to their legal obligation under Article 6(11) of Regulation (EU) 2022/1925 and to the re-use or further processing of that data by the third-party OSEs.[860]

(552) It also follows from Article 6(11) and recital 61 of Regulation (EU) 2022/1925 that the anonymisation of the end users' personal data must be achieved in relation to the third-party OSEs, which must not be able to identify the end user either by reversing the technical means to render data non personal for them or by other means available to them. By contrast, the end users' personal data does not have to be anonymous in relation to Alphabet, which might thus remain able to identify the end users. Such

---

855 Judgment of the Court of Justice of 19 October 2016, *Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779, paragraph 46.

856 Judgment of the Court of Justice of 4 September 2025, *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025-645, paragraphs 86 and 87. The judgment concerned the interpretation of the concept of "personal data" in Regulation (EU) 2018/1725, which encompasses the data protection rules applicable to the processing of personal data by the Union institutions, bodies, offices and agencies (OJ L 295, 21.11.2018, page 39). Nevertheless, the definition of "personal data" is the same in Article 3(1) of Regulation (EU) 2018/1725 as in Article 4(1) of Regulation (EU) 2016/679. According to recital 5 of Regulation (EU) 2018/1725, it is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules in those two regulations. Those two sets of provisions should, under the case law of the CJEU, be interpreted homogeneously, in particular because their schemes are equivalent.

857 *Ibid*, paragraph 75.

858 *Ibid*., paragraph 77.

859 *Ibid*., paragraph 84.

860 Joint EDPB and Commission guidelines on the interplay between DMA and GDPR, version for public consultation ("Joint Guidelines"), Doc ID […], paragraph 183. Said version of the Joint Guidelines is available at: https://digital-markets-act.ec.europa.eu/document/download/8ba0913f-2778-4a6d-9c58-10f8c7ead009_en?filename=Joint_COM-EDPB_GLS_interplay_DMA_GDPR_for_public_consultation.pdf

interpretation is in line with the case-law listed above that data that is personal for some entities (which can identify the data subjects) can be non-personal for others (which cannot identify the data subjects).

(553) To maximise the level of data quality and usefulness for third-party OSEs in line with the objective of enabling effective competition between OSEs pursued by Article 6(11) of Regulation (EU) 2022/1925 while ensuring that end users' Search Data is protected against possible re-identification risks, anonymisation (in relation to those third-party OSEs) should be achieved, in this specific context, by appropriate technical measures for alteration of the data, complemented by organisational, administrative and contractual measures to mitigate residual likelihood of identification.[861]

(554) In relation to technical measures for the alteration of data, these may include, for example, the removal of data liable to be used for the identification of the end user generating the Search Data (e.g., precise location of the end user, queries with words searched below a specific low number of times, and precise time and sequence of click data).[862]

(555) In relation to other measures aimed at mitigating the residual likelihood of identification, these may include, for example, contractual measures limiting onward sharing of the data and use of the data (including a prohibition to attempt to re-identify end users), security and access requirements (such as access control restrictions and data retention/storage measures), internal monitoring and supervision, independent auditing, incident reporting obligations (including, where appropriate, to the competent data protection supervisory authority), and appropriate remedial measures in the event of an established violation by the third-party OSE of the requirements set out in the contract (such as suspension of access or where appropriate, erasure of the data).[863] Besides, the measures imposed by the implementing act should also take into account changes of legal or factual circumstances, such as a merger or bankruptcy of third-party OSEs.[864]

(556) For end users' data not to be considered personal data for the third-party OSE and for other third persons that would reasonably be considered to be able to gain access or process the data (including unintended third parties[865]), the likelihood of identification should be insignificant, taking into account all the means reasonably likely to be used by the third party OSE and those other third persons to identify end users directly or indirectly.[866] In this regard, the assessment of whether identification is reasonably likely must take into account the legally binding conditions under which access to the ranking, query, click and view data is granted pursuant to an implementing act of the Commission, specifying the technical and contractual measures to be applied by the gatekeeper, insofar as those measures produce durable and verifiable effects.[867]

---

861 Joint Guidelines, Doc ID […], , paragraph 18.

862 Joint Guidelines, Doc ID […], , paragraph 188.

863 Joint Guidelines, Doc ID […], , paragraph 189.

864 Joint Guidelines, Doc ID […], , paragraph 189.

865 Unintended third parties designate any other person than the eligible third-party OSEs or the third parties with whom they have contracted in order to process Search Data on their behalf as processors (i.e. subcontractors).

866 Joint Guidelines, Doc ID […], , paragraphs 180, 181 and 185.

867 Joint Guidelines, Doc ID […], , paragraphs 181, 188 and 189.

4.4.2. Alphabet's approach

(557) This section provides an outline of Alphabet's anonymisation measures and the contractual terms for potential beneficiaries of Article 6(11) of Regulation (EU) 2022/1925, and their impact on the Google Search Data.

4.4.2.1. Anonymisation measures

(558) Alphabet anonymises the Google Search Data by applying two frequency thresholds: (i) a *k*-threshold for the query text, and (ii) an *m*-threshold to query text and metadata. The query text and metadata must meet both thresholds to be included in the Google Search Data.[868]

(559) ***k*-threshold**. The first threshold applies to query text for queries issued in the EEA. The query text refers to the input the end user enters in Google Search to perform an online search. A query text meets the *k*-threshold if at least 30 different, unique signed-in end users worldwide issued the same query text during the previous 13 months.[869]

(560) Alphabet counts query text towards the thresholds if the query produced a SERP. Alphabet does not count queries towards the thresholds that Google Search automatically corrects (e.g., triggering a prompt such as "*These are results for […]; search instead for […]*" at the top of the SERP) and do not produce results. Instead, Alphabet counts the corrected query text that produced results in those cases.[870]

(561) If the query text passes the *k*-threshold, Alphabet includes the query text on an allow list for five years, which means the query text does not need to meet the *k*-threshold in subsequent periods within those five years.[871]

(562) ***m*-threshold**. If the query text is on the allow list, the second threshold applies to the query text and metadata. The metadata that counts towards the threshold includes the viewed results on the SERP, the country, and device type. The query text and metadata meet the threshold if at least five different, unique signed-in users have issued the same: query text, result, country, and device type during the relevant quarter.[872]

(563) If the query text and metadata do not meet the threshold, Alphabet performs suppression and generalisation:[873]

(a) If the query text and metadata do not meet the m-threshold because of an individual device type, but they meet the threshold across device types (mobile phone and desktop), Alphabet releases the data suppressing the device type.

(b) Alphabet specifies the country only if the query text and metadata meet the *m*-threshold in the given EEA country.

(c) If the query text and metadata only meet the *m*-threshold at EEA-level, Alphabet releases the query text and metadata at that level. Alphabet includes this EEA-level data in the Google Search Data for any requested country.

(d) If the query text and metadata pass the m-threshold in at least one EEA country, Alphabet does not release the query text and metadata issued in other

868 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], , question 16.
869 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], , question 16.
870 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], , question 16.
871 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], , question 16.
872 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], , question 16.
873 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], question 16.

EEA countries in aggregated form even if the combined data from all EEA countries meets the m-threshold at the EEA level.

(564) If the query text and metadata do not meet the *m*-threshold in any of the above forms, Alphabet does not include them in the Google Search Data.[874]

(565) If the *k*-threshold and the *m*-threshold are met, Alphabet includes in the Google Search Data the query text and metadata of both signed-in and signed-out end users who input the query.[875]

(566) In addition, Alphabet performs a recovery mechanism for query text that has not passed the *k*-threshold. Alphabet includes in the allow list misspelled query text that is at most one edit distance away from the correct spelling that meets the *k*-threshold. However, for Alphabet to include it in the Google Search Data, the misspelled query text and metadata must both meet the *m*-threshold.[876]

(567) On 3 March 2026, in the course of the specification proceedings, Alphabet presented a high-level alternative proposal under which it would not share one general dataset to comply with Article 6(11) of Regulation (EU) 2022/1925, but would instead share several datasets that are optimised for specific use cases, such as a dataset sharing more information on queries for the purpose of query analysis.[877] Alphabet has not provided any details as to this potential alternative, and it does not currently offer such datasets. Alphabet has been aware of third parties' criticism of the limited quality and usefulness of its data licencing program since shortly after it launched this program,[878] yet this was the first time – eight weeks before the legal deadline for the Preliminary Findings in the present specification proceedings – that Alphabet mentioned the possibility for another approach, which it argues would have the potential to safeguard more utility. While the Commission has received insufficient detail on the alternative proposal to assess it fully, Alphabet's proposal for use-case-specific datasets suffers from the shortcoming that Alphabet can control for which use cases it makes Search Data available. The number of use cases for the Search Data is large, varies across recipients, and constantly evolves. Furthermore, how beneficiaries use the Search Data can be competitively sensitive, as different online search engine providers pursue different strategies to optimise their services. They must not be in a position where they divulge their intended use case to Alphabet in the hope that Alphabet makes a suitable dataset available. Finally, Alphabet did not develop this proposal further after the Preliminary Findings.

(568) On 18 May 2026, after the adoption of the Preliminary Findings, Alphabet submitted an alternative anonymisation proposal. The proposal consists of five parts:

(a) **Generalising rare queries to the semantically-nearest query that passes threshold *k*.** Alphabet proposes to apply the same k threshold of 30 to the full query text as in its current approach. However, it would not suppress queries that do not meet the threshold but apply LLM technology to find the semantically closest query among queries that passed the *k*=30 threshold and would then align the query with the nearest query. Alphabet would additionally release the similarity score for each query that did not pass the threshold.

---

874 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], question 16.

875 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], question 16.

876 Alphabet's reply to question 16 of RFI 11 of 12 November 2025, Doc ID […], question 16.

877 Alphabet's presentation "Anonymizing the dataset" of 3 March 2026, Doc ID […].

878 See Alphabet's response to [market participants], Doc ID […], and to [market participants]'s feedback, Doc ID […].

(b) **Replacing timing of attention signals with placeholders.** Alphabet proposes to replace the exact timing of interactions with placeholders (*served, viewed, considered and clicked*), instead of releasing unaltered interaction data.

(c) **Metadata generalisation.** Alphabet proposes metadata groups of 1,000 end users. Additionally, it proposes a separate threshold of five signed-in end users to the combination of the (generalised) query text and metadata (location, device type and language). It also proposes a third separate threshold of two signed-in end users for the combination of URL and metadata, based on URL impressions.

(d) **No mini-session grouping**. Alphabet's proposal does not group queries into mini-sessions, as is the case for the Commission's measures (see section 4.4.4.1.2.1.5).

(e) **No personalised ad URLs.** Alphabet's proposal suppresses all ad URLs.

Alphabet argues that this proposal increases privacy protection while maintaining utility. The Commission analyses this alternative proposal in the section 4.4.2.3 below.

4.4.2.2. Contractual terms

(569) Applicants that seek access to the Google Search Data must enter into a contract with Alphabet. The standard contract imposes the following main contractual terms on data recipients:[879]

(a) **Purpose of use restriction:** recipients may only use the Google Search Data to optimise the value of their online search engine for end users.

(b) **Sharing data with third parties:** Recipients may share the Google Search Data with authorised vendors, provided they obtain Google's prior written consent, carry out adequate due diligence of the vendor, impose the same contractual restrictions and obligations on the authorised vendor, and retain oversight.

(c) **Review and verification:** the recipient must allow Google to review the recipients accessing of the Google Search Data to verify compliance with the contractual terms.

(d) **Data retention:** recipients must delete the Google Search Data within one year of the date on which it was downloaded.

(e) **Audit**: recipients must agree to an audit by an independent auditor of Google's selection to ensure compliance with the contractual terms.

(570) Recipients must also comply with Alphabet's Data Security Requirements ("**DSR**"). The DSR imposes requirements on the recipient's handling and storage of the Google Search Data:[880]

(a) **Physical controls:** the recipients must maintain physical controls to secure the relevant facilities, such as perimeter and interior barriers and access controls.

(b) **Technical controls:** recipients must implement technical controls such as on-cloud processing to protect against security issues in office or work from home

879 Alphabet's Search Data Agreement, Doc ID […].

880 Available on: https://business.safety.google/datasecurityrequirements/, Doc ID […], last accessed on 20 February 2026.

environments, limiting admin rights to no more than 10 senior employees, access control policies, logging, etc.

(c) **Personnel training:** recipients must provide confidentiality and information security training to personnel that has access to the Google Search Data.

(d) **Encryption:** recipients must encrypt Google Search Data to a reasonable standard when transferring or storing.

(e) **Assessments and audits:** recipients must submit to assessments of compliance with the contractual terms, third-party penetration testing, perform self-assessments, and submit to audits of the architecture, systems processes and procedures relevant for protection of the Search Data.

(f) **Security incidents**: recipients must maintain a security incident response programme and notify Google of incidents.

4.4.2.3. Impact on the data shared

(571) Recital 61 of Regulation (EU) 2022/1925 explains that Alphabet must anonymise end user data without substantially degrading the quality or usefulness of the data. When selecting among various possible ways of achieving anonymisation of the Google Search Data, Alphabet must select the one that preserves the most quality and usefulness of the data.[881] Alphabet's anonymisation approach removes a large amount of data from the Google Search Data, thereby significantly degrading data quality. The Commission considers that Alphabet has not considered all available means to anonymise the Google Search Data, and that alternatives that have a less detrimental impact on data quality and usefulness are available.

(572) Alphabet's anonymisation measures remove approximately [90-100]% of unique queries and [30-40]% of query volume in the EEA over a quarterly release period of the dataset.[882] Third parties indicate that this extent of data removal significantly degrades the quality of the data.[883] The data that is removed from the dataset are the rarer queries, also called the "long tail" of queries. These are most valuable to beneficiaries, as they are less likely to have data on these queries, whereas Alphabet has data on them due to its scale.[884] This means that not only does Alphabet's anonymisation proposal remove the vast majority of unique queries, the queries removed are also those that would be most valuable to third-party online search engines to optimise their services – further aggravating the loss of data quality and usefulness. In this regard, a third party states: "*[i]ncluding the long tail will vastly improve the usefulness of the data, as smaller competitors do not see these queries at all today due to their volume.*"[885]

(573) There are several elements of Alphabet's anonymisation approach that drive the large loss of data quality and usefulness.

---

881 Joint Guidelines, Doc ID […], paragraph 180.

882 Alphabet's reply to RFI 2 of 22 December 2023, Doc ID […], question 1c.

883 See https://spreadprivacy.com/investigate-google-dma/, last accessed on 9 March 2026, Doc ID […], [market participant]'s submission of 17 January 2024, Doc ID […], and agreed minutes of a meeting with [market participant]on 30 September 2024, Doc ID […], paragraph 5.

884 See [market participant]'s submission of 5 December 2023, Doc […], [market participants]'s reply to RFI 1 of 18 November 2025, Doc ID […], [market participant]'s submission of 17 January 2024, Doc ID […], agreed minutes of a meeting with [market participant]on 30 September 2024, Doc ID […], paragraph 5, agreed minutes of meeting with [market participant]on 26 November 2025, Doc ID […], and [market participant]submission of 4 September 2025, Doc ID […], paragraph 9.

885 [Market participant]'s Feedback on Compliance with Article 6(11), DMA (Click-and-Query Data) of 5 December 2023, Doc ID […].

(574) **First,** Alphabet's anonymisation measures aim to remove all personal data from query text – even if the personal data is not associated with the end user that issued the query.[886] In contrast, Article 6(11) of Regulation (EU) 2022/1925 only requires anonymisation of end-user personal data, but not of personal data of other identifiable individuals, to which Regulation (EU) 2016/679 still applies.[887] [888] Relatedly, Alphabet does not clearly outline an adversarial model that takes into account the practical circumstances of data sharing under Article 6(11) of Regulation (EU) 2022/1925.

(575) **Second**, Alphabet's *k*-threshold applies to the entire query text. This means that queries that consist of common words put in an order that is not searched very often are filtered out, even if these queries are not problematic. This anonymisation step alone (i.e., without considering the other steps that Alphabet applies), removes the vast majority of the data: [90-100]% of unique queries and [30-40] of query volume are searched by fewer than 30 users in the EEA, which is the level of Alphabet's threshold.[889] However, even choosing a far lower threshold removes a large amount of data: a *k*-threshold of 2 removes approximately [80-90]% of unique queries.[890] This shows that applying thresholds over the full query text has a severe impact on data quality and usefulness, no matter which threshold is chosen. For this reason, [market participant] argues that anonymisation of queries should focus on removing personal identifiers, like phone numbers, user ids and passwords, rather than applying thresholds to the full query text.[891]

(576) **Third,** Alphabet's additional anonymisation measures further deteriorate data quality and usefulness. Alphabet applies an *m*-threshold to anonymise metadata related to each query. However, Alphabet's *m*-threshold does not only apply to the query metadata, but also to the query text – despite the query text already being anonymised with the *k*-threshold. This overlap drives significant additional data removal. This step taken in isolation removes more than [90-100]% of query-metadata combinations.[892] In contrast, when sharing queries with website owners on Google Search Console to assess the performance of their websites, Alphabet only uses a query threshold without metadata thresholding,[893] showing queries that led to as little as one impression or click on one result.

(577) **Fourth**, there is concrete indication that Alphabet's anonymisation approach removes a large amount of data that does not constitute end user personal data (so called "false positives"). Analysis of a representative sample of queries taken from

---

886 Alphabet's presentation of 11 December 2024, "*Anonymizing Google Search data*", Doc ID […], slide 14, presenting the study "*Privacy Expert Report on DMA Art. 6(11) Google Search Data Sharing*" authored by Dr. Chris Culnane & Prof. Ben Rubinstein, Doc ID […].

887 See paragraph (551) and the Joint Guidelines, Doc ID […], paragraph 183.

888 Alphabet's external expert risk assessment also encompasses personal data from any individual, rather than being limited to the end user who issued the query. See Alphabet's study "Privacy Expert Report on DMA Art. 6(11) Google Search Data Sharing", Section 1, authored by Dr. Chris Culnane & Prof. Ben Rubinstein, Doc ID […].

889 Alphabet's reply to RFI 11 of 12 November 2025, Doc ID […], questions 7 and 8. Alphabet performed the analysis over 10 months of search data, rather than 13 months. However, the result is unlikely to change materially when considering 13 months, which is the time horizon of Alphabet's *k*-threshold.

890 Alphabet's response to RFI 11 of 12 November 2025, Doc ID […], question 7. Alphabet performed the analysis over 10 months of search data, rather than 13 months. However, the result is unlikely to change materially when considering 13 months, which is the time horizon of Alphabet's *k*-threshold.

891 See https://spreadprivacy.com/investigate-google-dma/, Doc ID […], last accessed on 9 March 2026.

892 Alphabet's reply to RFI 11 of 12 November 2025, Doc ID […], question 21.

893 Alphabet's reply to RFI 11 of 12 November 2025, Doc ID […], question 22: [description of Alphabet's internal interal system processes]

one week of search data from Ireland shows that [90-100]%[894] of reviewed search records that Alphabet removed from the Google Search data before sharing did not contain end user personal data.[895] [896] The analysis simulated the scenario in which beneficiaries receive the data and are restricted from combining it with other datasets.[897] [898] Additionally, the assumptions regarding what constitutes end-user personal data were conservative, meaning that when there was any reasonable doubt that a query could relate to an end user, it was considered as personal data for the purpose of the analysis, which reduced the number of observed false positives (i.e., the error rate of [90-100]% is likely even higher).[899] Overall, this analysis shows that Alphabet removes significantly more data from the Google Search Data than is strictly necessary, which in turn has a significant negative impact on the quality and usefulness of the dataset for potential beneficiaries.[900]

(578) Alphabet criticises the Trilateral report which demonstrates the false positives in Alphabet's anonymisation approach for adopting a flawed definition of personal data, a lack of balance between false positives and false negatives, and for methodological errors.[901] However, this critique misrepresents the analysis performed in the report. Contrary to what Alphabet purports, the Trilateral report took a practical approach to whether a record is re-identifiable – namely whether the query can be used to re-identify the end user that issued it. The report took conservative assumptions in this regard, assuming that personal data belongs to an end user even in cases where this was uncertain (which is unlikely to hold in practice, see recital (750)). Furthermore, Alphabet appears to misunderstand the purpose of the report. Alphabet claims that the report does not balance the importance of false positives and false negatives correctly. However, the report is simply an exploratory analysis of the Google Search Data and Alphabet's anonymisation approach and does not take any position on the appropriate balance between false positives and negatives. The design of the Commission's technical anonymisation measures did not "follow" the analysis in the report – as Alphabet tries to suggest.[902]

(579) **Last**, there are several other aspects of Alphabet's anonymisation approach that degrade data quality and usefulness of the Google Search Data, and where

---

894 [90-100]% (with a 95% confidence interval between [90-100]% and [90-100]%) is the weighted average false positive rate estimated in the consultant's report across search records (query-result pair) removed due to Alphabet's *k*-threshold, *m*-threshold, or both.

895 Rexilience's protocol "Google Search Dataset Privacy Protocol", Doc ID […]. This protocol was followed by Trilateral to identify end user personal data in a representative sample of Google Search data in their report "Support for Art. 6.11. Click & Query data obligation. Task 2 – Data Analysis", Doc ID […].

896 Trilateral's report "Support for Art. 6.11. Click & Query data obligation. Task 2 – Data Analysis", section Conclusion, Doc ID 1918. To arrive at its conclusion, Trilateral wrote code to extract and analyse a representative sample from the week of search data from Ireland, and manually annotated that sample. The annotations and code may be found in the Google Cloud environment ([Alphabet's internal system name]]) that Alphabet provided to the Commission's contractor Trilateral to perform the study, specifically in the directory with address: [address].

897 Rexilience's protocol "Google Search Dataset Privacy Protocol", Doc ID […].

898 Trilateral's report "Support for Art. 6.11. Click & Query data obligation. Task 2 – Data Analysis", section Scope and Limitations, Doc ID […].

899 Trilateral's report "Support for Art. 6.11. Click & Query data obligation. Task 2 – Data Analysis", section Scope and Limitations, Doc ID […].

900 Trilateral's report "Support for Art. 6.11. Click & Query data obligation. Task 2 – Data Analysis", section Executive Summary, Doc ID […].

901 Annex 5 to Alphabet's response to the Preliminary Findings, Doc ID […].

902 Annex 5 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraph 11.

alternatives could be available that have a less adverse impact on data quality and usefulness. These include:

(a) **Aggregation of data:** Alphabet aggregates records by query and metadata and provides only aggregated statistics about click and ranking information (see sections 4.3.2.2.5 and 4.3.2.4). Record-level ranking data provides important nuance that is necessary when optimising online search engine services, and is therefore important to data quality and usefulness.[903] The Commission considers that it is possible to share record-level data while anonymising end user personal data (see section 4.4.3).

(b) **Release frequency:** Alphabet releases data every quarter at the end of the subsequent quarter with a timestamp granularity of three months, which makes the data four and a half months old on average (see section 4.4.2.1). Alphabet argues that this latency does not affect training of online search engines as beneficiaries can train their online search engines with data that they own that is older than three months.[904] However, third parties have indicated that receiving old data means the data is stale by the time it is received, and therefore less useful to optimise search services. Third parties explain that fresh data is for instance relevant to inform crawling strategy and maintain signals such as page quality.[905] The Commission considers that it is possible to share data more frequently while maintaining the anonymity of end user data (see section 4.4.3).

(c) **Location granularity:** Subject to the *m*-threshold, Alphabet includes the country where the end user issued the query (see section 4.4.2.1). However, the Commission considers that Alphabet has not considered approaches that provide location information with a higher level of data quality and usefulness while maintaining end user privacy. For instance, Alphabet's approach does not account for the varying population densities: Malta and Germany are at the same level of generalisation protection despite vastly different sizes and population. This means that at the very least, Alphabet can provide more detailed location information for larger countries such as Germany. Alphabet's approach also impedes the ability of beneficiaries to train their online search engines with location-based queries (e.g., "*coffee near me*").[906] Third parties indicate that granular location information is critical to improve their online search engines.[907] The Commission considers that it is possible to provide more granular location information while maintaining the anonymity of end user data (see section 4.4.3).

(d) **Session-level data:** Alphabet removes any type of session data from the Google Search Data (see section 4.3.2), e.g., linked queries with their associated results and metadata that could capture an end user task or time interval when using the online search engine. While long sessions may pose a

---

903 See https://spreadprivacy.com/investigate-google-dma/, Doc ID […]1, last accessed on 9 March 2026, agreed minutes of a meeting with [market participant]on 30 September 2024, Doc ID […], paragraph 6.

904 Alphabet's reply to RFI 1 of 28 November 2023, Doc ID […], question 20.

905 Responses to RFI 1 of 18 November 2025 by [market participant], Doc ID […], [market participants], Doc ID […], [market participant], Doc ID […], [market participant], Doc ID […], [market participant], Doc ID […], and [market participant], Doc ID […].

906 Agreed minutes of a meeting with [market participant]on 30 September 2024, Doc ID […], paragraph 5.

907 [Market participant]'s submission of 17 January 2024, Doc ID […], [market participant]'s responses to RFI 1 of 18 November 2025, Doc ID […], agreed minutes of a meeting with [market participant]on 21 January 2026, Doc ID […], and agreed minutes of a meeting with [market participant]on 17 February 2026, Doc ID […].

privacy risk, Alphabet has not proposed a suitable privacy measure to release shorter end-user sessions that can support beneficiaries in improving their algorithms, e.g., query understanding. The Commission considers that it is possible to share limited session-level data while maintaining the anonymity of end user data (see section 4.4.4.1.2.1.5).

(580) Alphabet's alternative anonymisation proposal of 18 May 2026 differs from its current approach, as it generalises queries that do not meet the *k*-threshold, rather than suppressing them. However, Alphabet's alternative proposal still goes far beyond what is required to alter the Search Data to mitigate the risk of re-identification without substantially degrading the data quality and usefulness. As potential data recipients put it: "*Alphabet's 22 May anonymisation counter-proposal destroys utility and would relocate control over data quality to Alphabet.*"[908] The measures in the present Decision have a less detrimental impact on data quality and usefulness, while still meeting the anonymisation requirement of Article 6(11) of Regulation (EU) 2022/1925.

(581) There are several ways in which Alphabet's alternative anonymisation proposal would have a detrimental impact on data quality and usefulness:

(a) Alphabet claims that the query generalisation method would release (only) [20-30]% of unique queries in non-generalised form based on one week of Irish data. However, this figure is misleading. When considering 13 months of EEA data, which is the full scope of data that recipients can acquire under the allowed retention period, fewer than [0-10]% of queries would be provided in their original form.[909] While the remaining queries would be provided in generalised form, this generalised query is designed to maintain the intent of the query – not the query as originally entered by the end user. One of the key use cases for the Search Data, as set out in recital (18)(d), is to develop models for query understanding. Even if Alphabet's generalisation method would accurately maintain query intent, by sharing the distilled query intent rather than the original query the Search Data will no longer serve this use case.

It is also questionable that query intent would always accurately be maintained[910] – which may actively hurt the optimisation of beneficiary search services, as they would be training on inaccurate data. This is particularly the case for generalised queries that receive a high similarity score despite capturing intent of the original query poorly. The data recipient has no way of knowing that this record conveys an inaccurate data signal, due to the black-box "similarity" scoring of Alphabet's embeddings. Queries with low similarity scores present a problematic choice for data recipients too: they must either remove a large part of the available data – which they have paid for – when training their models or train their models on data they know is inaccurate.

(b) The metadata generalisation would cover both the query text and result URLs in two separate generalisation steps. This means that at least five users must have issued the same (generalised) query text in the same location on the same device type. Because many query texts are issued by very few users ([80-90]%

---

908 [Market participants]written submission of 9 June 2026, page 2.

909 This is because rarer queries, which do not pass the threshold of 30, accumulate over time. See Alphabet's reply to RFI 11 of 12 November 2025, Doc ID […], question 7.

910 For instance, the query text "*bus from dundrum to red cow"* is generalised to "*dundrum to red cow*", which is materially different despite having a very high (0.97) similarity score.

of queries over 13 months worldwide are issued by a single user)[911], this drives a large amount of metadata generalisation. Considering daily data releases, only [0-10]% of unique queries would be released without any metadata generalisation. [80-90]% of unique queries would be subject to extensive generalisation and would be released without *any* of the crucial metadata: no indication of location (beyond that the query was issued in the EEA), no indication of device type, and not even an indication of the query language (which may have changed in the process of query generalisation).[912] As seen, these metadata attributes are of crucial importance for recipients to optimise their search services (see section 4.3.2). The second metadata generalisation step, which covers result URLs, further aggravates the situation. The URL generalisation step would suppress more than half ([50-60]%) of all result URLs in the data.[913] Without result URLs, recipients cannot optimise their crawling and indexing strategy, as they would have no indication which URLs to crawl and index. They would also not be able to optimise their retrieval and ranking systems with the Search Data, as in the majority of cases, the result would be fully suppressed.

(c) The placeholders that replace interaction data give no indication of interaction durations. This means that recipients would not be able to tell the level of engagement of an end user with a result – was it considered very briefly, or for a longer time? These are important signals to determine the quality of a result (see section 4.3.2.2).

(582) Nevertheless, in the present Decision the Commission has adopted certain revisions to the technical measures contributing to ensure anonymisation that are in line with Alphabet's alternative anonymisation proposal. First, ad URLs are now suppressed (see recital (596)(h)). Second, the metadata groups have increased to 1,000 (as an absolute minimum, and because the minimum location granularity has been updated to a much coarser level, most users would fall in significantly larger metadata groups, see recital (604)) – in line with Alphabet's alternative proposal. Third, the measures now coarsen interaction data (see recital (605)), albeit in a different way than suggested by Alphabet.

(583) In summary, the Commission considers that Alphabet has not considered all appropriate means to anonymise the Google Search Data, and that alternatives technical means that have a less detrimental impact on data quality and usefulness are available.

4.4.3. The gatekeeper's view

(584) Alphabet argues that the anonymisation measures that the Commission proposed in the Preliminary Findings give rise to serious risk of reidentification. Alphabet submits that this is confirmed by a red-teaming exercise it performed on a sample of data, which surfaced potential examples of re-identification.[914]

(585) First, Alphabet argues that the re-identification risk associated with the Search Data is inherently high, as the dataset is vast, open-ended and complex and contains a high proportion of queries that are unique to a single user. Alphabet also argues that a large range of other data that can be linked with the Search Data is available. Alphabet argues this gives rise to several risks:

911 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 111.
912 Alphabet's reply to RFI 16 of 22 May 2026, Doc ID […], question 3.
913 Alphabet's reply to RFI 20 of 22 June 2026, Doc ID […], question 1.
914 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 99-104.

(a) The open-ended nature of the Search Data means that queries can cover any number of topics, including sensitive topics, that render an end-user identifiable.[915]

(b) The high proportion of unique queries in the Search Data allows singling out of users, and the queries may reveal additional information about the user as well.[916]

(c) Recipients of the data have access to auxiliary datasets that can be combined with the Search Data – notably their own search data. Recipients can link this data using different methods, e.g., looking for identical or related queries submitted to the recipient and Google Search.[917]

(586) Second, Alphabet argues that Article 6(11) of Regulation (EU) 2022/1925 requires that any shared data must be anonymised to the standard of Regulation (EU) 2016/679. In that regard, Alphabet argues anonymisation is an objective concept, subject to a strict standard requiring to render identification practically impossible.[918] Alphabet argues that anonymisation is not about recipient's incentives or interests to actually identify users.[919]

(587) Third, Alphabet argues that the technical anonymisation measures proposed in the Commission's Preliminary Findings do not rely on standard, well-tested and recognised anonymisation techniques, and leave the Search Data exposed to a high risk of re-identification, due to the following main issues:

(a) The query suppression proposed by the Commission does not protect users against re-identification, as it controls for rare words or entities, but does not consider that combinations of common words can convey identifying information.[920] Furthermore, Alphabet argues that the additional length-based threshold does not protect against re-identification and is arbitrary and unprincipled. Alphabet argues that personal data is not limited to long queries, and that the threshold which excludes 5% of the longest queries per language changes over time as query length is growing, which means that longer queries will be revealed over time.[921]

(b) The metadata generalisation step does not apply to the combination of a given query and its metadata, leaving unique queries distinguishable within a metadata group.[922] Alphabet additionally argues that upleveling only some metadata fields does not provide meaningful protection, as the combination of query text with the remaining metadata attributes allows singling out of users, particularly with the threshold set at 50.[923] Moreover, Alphabet argues that the metadata generalisation ignores relevant metadata fields that are quasi-identifiers, such as free result URLs, ad URLs, user behaviour (interaction) data, and the query input format. Alphabet argues that those fields can be used to infer the metadata fields that are generalised.[924]

---

915 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 107-110.
916 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 111-118.
917 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 119-134.
918 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 135-147.
919 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 290-294.
920 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 153-162.
921 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 163-172.
922 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 177-187.
923 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 188-194.
924 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 195-214.

(c) The proposed technical anonymisation measures do not protect users against re-identification through re-sessionising queries. Alphabet argues this is the case because the data shared is granular and allows to link individual queries by topic.[925] Furthermore, Alphabet argues the proposed mini-sessionisation can lead to disclosure of longer sessions that cover multiple unrelated topics, further enabling re-sessionisation.[926]

(d) The Commission did not conduct testing of its proposed technical anonymisation measures. Alphabet argues that the testing the Commission performed is insufficient, and that the Commission had access to a sample dataset for long enough to test the measures.[927]

Alphabet argues that the results of the Commission's public consultation confirm these shortcomings.[928]

(588) Fourth, Alphabet argues that contractual measures are not a permissible way to compensate for re-identification risks remaining after application of the technical anonymisation measures. Alphabet argues that this is the case for the following reasons:

(a) This approach conflicts with the requirement to share Search Data in anonymised form set out in Article 6(11) of Regulation (EU) 2022/1925. Alphabet argues that the anonymisation measures proposed in the Commission's Preliminary Findings do not irreversibly alter data such that it is no longer identifiable, and do not achieve anonymity. Alphabet argues that contractual measures do not change that.[929] That claim aligns with the expert legal opinions on anonymisation commissioned by Alphabet of 18 November 2024 and 25 March 2026 arguing that since the definition of anonymised data under Regulation (EU) 2022/1925 is consistent with that of Regulation (EU) 2016/679, "*search data subject to the sharing obligation which constitutes personal data* 'shall be anonymised' *before being shared*", *which presupposes that the dataset has already been rendered anonymous*" (emphasis added).[930] Alphabet also submits that the fact that the Commission requires Alphabet to impose the specified contractual measures would change nothing, since the specification measures only bind Alphabet and do not bind recipients of the Search Dataset.[931]

(b) The reliance on contractual measures violates the right to informational self-determination of end users. Alphabet argues that as Regulation (EU) 2016/679 no longer applies to the shared Search Data despite users still being identifiable, they will be deprived of their rights, including information rights, their rights of access, rectification, erasure and objection and protections in connection with transfers outside the EEA, under that Regulation. Alphabet argues that these rights would be replaced by a contract to which the end users are not a party, violating their right to informational self-determination.

925 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 215-220.
926 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 221-227.
927 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 228-234.
928 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 235-236.
929 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 243-252.
930 Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], page8 and 10. See also initial Alphabet's Expert Opinion: the Anonymisation Requirement under Article 6(11) of the DMA in the context of the GDPR of 18 November 2024, Doc ID […], paragraphs 4, 30 and 38.
931 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 251.

Alphabet further argues that the Preliminary Findings explanation that the Search Data would become personal data again in the case of a breach of the contractual measures would leave the classification of Search Data in an indeterminate state. Alphabet argues that end users that replied to the Commission's public consultation also echoed concerns for their fundamental rights.[932]

(c) Even if contractual measures were a permissible way to address the residual re-identification risk remaining after application of the technical measures, Alphabet argues the residual likelihood of re-identification is too high in this case. As set out in the previous recital, Alphabet argues that the proposed technical anonymisation measures leave the Search Data exposed to a high risk of re-identification.[933]

(d) Alphabet also argues that the Preliminary Findings ignore that recipients are search engines that have their own search data, which they will inevitably combine with the Search Dataset creating re-identification risks that contractual measures cannot address given the high overlap between recipients' and Google's users.[934]

(e) Alphabet submits that the reliance on recipients' incentives to abide by the contract is misplaced, as it is incompatible with the concept of anonymisation, and has no factual basis as recipients have significant incentives to reidentify users.[935] This claim also relates to the expert legal opinions on anonymisation commissioned by Alphabet of 18 November 2024 and 25 March 2026 according to which "[third-party OSEs] *may have a commercial interest in re-identifying the anonymised data*", considering the value and sensitivity of Google Search Data.[936]

(f) Alphabet argues further that neither the Commission nor Alphabet have any good means to detect re-identification events that will take place in breach of contractual promises and that even if a breach were discovered, the contracts do not foresee consequences that are capable of dissuading breaches so that there is no basis for assuming that the value of continuing with the contract would necessarily outweigh the value of a breach.

(g) Furthermore, Alphabet argues that contracts are bilateral and do not bind third parties that may obtain the data, for instance through breaches. They also cannot prevent foreign governments to seize the data through administrative or judicial measures as several of the intended recipients are established in the US and are subject to US jurisdiction. Alphabet further argues that since the Preliminary Findings permit sharing with third-party providers, they open the door to long processing chains and sharing with many third parties that amplify the risk of leaks.[937]

---

932 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 253-267.

933 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 268-275.

934 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 121-128 and 276-281.

935 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 284-302.

936 Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], page 18. See also initial Alphabet's Expert Opinion: the Anonymisation Requirement under Article 6(11) of the DMA in the context of the GDPR of 18 November 2024, Doc ID […], paragraph 38.

937 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 282-283.

(h) Alphabet argues that the harm from a breach for users would be serious and irreparable, meaning that the reliance on contractual measures is legally inappropriate and ineffective.

(i) Finally, Alphabet argues that since the Preliminary Findings expressly stress that "*the Search Dataset inevitably includes personal data relating to individuals other than end users*"[938], this means that end user data remains personal data as it cannot be possible for end user data to be anonymised but for non-user data to remain personal data.[939]

(589) Fifth, Alphabet argues that the Commission's Preliminary Findings prioritise the interests of a small group of recipients over appropriate anonymisation, by prioritising data quality and usefulness over protection of personal data. Alphabet argues that the Commission did not properly test what measures are needed to protect end user data and that the Commission's restricted the analyses of its experts.[940]

(590) Sixth, Alphabet argues that an audit mechanism is a box-ticking exercise that does not offer any practicable way to detect contractual breaches as it focuses on whether controls are in place at a particular point in time, rather than whether those controls are operating effectively on an ongoing basis.[941]

(591) Seventh, Alphabet argues that the Commission's Preliminary Findings specify vague and open-ended security measures which significantly dilute the protection compared to Google's Data Security Requirements applicable under Google's licencing agreement, as they afford recipients broad flexibility to determine their own measures. For example, they fail to specify encryption standards, access controls, logging and monitoring requirements, patching and vulnerability management, personnel training and supervision, and incident response procedures and any right for Alphabet to be informed of data breaches.[942]

(592) Eighth, Alphabet argues that by imposing this highly detailed and prescriptive framework, the Commission must acknowledge its responsibility as a controller over the search data.[943]

4.4.4. Measures

(593) The Commission's measures ensure anonymisation of end users' personal data in the Search Data by mitigating the risks of end users' re-identification to an insignificant level through:

(a) **Technical measures**: these measures alter the Search Data and play a prominent role to mitigate the risk of re-identification of end users without substantially degrading the data quality and usefulness (the Search Data after the application of technical measures is referred to as the "**Search Dataset**"). These measures are outlined in section 4.4.4.1.

(b) **Contractual measures**: the contractual measures complement the technical measures and further mitigate the residual risks of re-identification of end users.[944] These measures are outlined in section 4.4.4.2.

938 Preliminary Findings, Doc ID […], paragraph 521.
939 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 301.
940 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 303-313.
941 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 575-578.
942 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 584-590.
943 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 591-598.
944 Joint Guidelines, Doc ID […], paragraph 181.

4.4.4.1. Technical measures

(594) The Commission's technical measures alter the Search Data to reduce the overall re-identification risk in four steps:

(a) **Attribute suppression**. The first step removes identifying attributes from each search record.

(b) **Query suppression**. The second step consists of three parts:

(1) ***Allow list creation***: Determines whether queries pass an entity-based threshold based on 13 months of EEA data and creates an allow list.

(2) ***Length-based threshold determination***: Determines the threshold on query length (a one-time operation).

(3) ***Suppression***: Suppresses queries when they are not included in the allow list or do not meet the length-based threshold.

(c) **Metadata generalisation**. The third step applies metadata generalisation on search records that contain allow listed queries.

(d) **Mini-sessionisation**. The fourth step groups records into "mini-sessions".

4.4.4.1.1. Measures

(595) Alphabet must share the Search Data daily and at record level in random order. Each input record must contain a query text with metadata and must successfully meet the Commission's technical measures to be included in the Search Data. The technical measures consist of the following steps:

(596) **Attribute suppression**. For each record, the following attributes are removed ((a) to (k)) and replaced ((l)).

(a) Any end user identifier, i.e. any direct identifier assigned to a user or user session, such as Google account identifiers (e.g., account IDs, usernames), whether the user was signed in, and other associated direct identifiers (e.g., IP addresses, device IDs).

(b) The timestamp of the query. For the avoidance of doubt, the day of the query must remain available.

(c) Information about the size (height and width) of modules and results.

(d) Information about the distance from each module or result to the top of the SERP.

(e) Information about the share each module or result occupies of the user's viewport.

(f) The access point.

(g) The input format.

(h) Ad URLs. For the avoidance of doubt, the existence of an ad and interaction data related to that ad shall be maintained.

(i) Advanced filters applied to a query.

(j) Results that are Google services which directly include personal information saved in an end user Google account (e.g., Google Maps results with directions to or from home) or the end user's exact location (e.g., Google Maps result

with directions). Alphabet shall submit a list of such result types to the Commission for approval within the time limit specified in section 4.6.4.

(k) Within sessions in AI Mode, any queries after the initial query (only the initial query of an AI Mode session should be provided).

(l) Queries in the form of images must be replaced with a placeholder query. For queries that combine images and text, only the image must be replaced with a placeholder query. The text must not be suppressed.

(597) **Allow list creation:** Alphabet must generate and update monthly an allow list of words appearing in search queries from signed-in end users using the past 13 months of EEA search data employing the following procedure:

(a) Alphabet must split the original query text of each search record into *entities*:

(1) Alphabet must use personal data detectors to detect addresses, names, phone numbers, location coordinates, IBAN numbers, credit card numbers and other forms of well-known identifiers and resolve them to standard formats.

(2) Alphabet must split the rest of the query, which has not been detected as personal data, into words based on whitespace, not counting whitespaces between two digits.

For example, the query "*john doe 200 wetstraat brussel 04 12 34 56 78 communications department*" could be split into "*john doe*" (flagged by the full name detector), "*200 wetstraat brussel*" (flagged by the address detector), "*04 12 34 56 78*" (flagged by a phone number detector), "*communications*", and "*department*" (single words).

(b) For each entity, Alphabet must count the number of unique signed-in end users who submitted queries containing the entity in the past 13 months in the EEA.

(c) Alphabet must add an entity to an allow list for five years if the entity is included in queries issued by more than 50 (w) signed-in end users.

(598) **Length-based thresholds determination**: Based on queries issued in 2025 by both signed-in and signed-out users in the EEA, Alphabet must compute a length-based character threshold (c) as follows:

(a) For each inferred language in which a query text has been issued, find the value of threshold c so that 95% of unique queries with that inferred language have fewer than c characters.

(599) **Query suppression:** Every day, Alphabet must apply the following procedure on each search record generated by signed-in and signed-out end users in the past 24 hours in the EEA:

Alphabet must remove the entire search record from the Search Data if the modified query (see definition in paragraph (211)(a)(2)) does not meet either of two conditions:

(a) **Entity-based threshold**: Alphabet must split the query text into entities (as described in paragraph (597)(a)) and determine whether all entities are in the allowlist.

(b) **Length-based threshold:** Alphabet must check whether the query text is shorter than the length threshold of c characters (see paragraph (598)) for the query's associated inferred language.

(600) If the initial query text (see definition in recital (211)(a)(1)) is different from the modified query text, Alphabet must check whether the initial query text meets the two thresholds. If the initial query text does not meet the two thresholds, the initial query text is removed from the search record; otherwise, Alphabet must add the initial query text as a data field to the corresponding search record.

(601) If the SERP contains query modifier text, Alphabet must check whether the query modifier text meets the two thresholds. If the query modifier text does not meet the two thresholds, the query modifier text is removed from the search record; otherwise, Alphabet must add the query modifier text as a data field to the corresponding search record.

(602) **Metadata generalisation:** For queries that pass query suppression, Alphabet must apply metadata generalisation to each search record. The attribute subject to generalisation is the location. The timeframe for metadata generalisation is that of the data release, i.e. 24 hours.

(603) Alphabet must share the location data of the end user using the third level of the EU Nomenclature of territorial units for statistics (NUTS 3).[945]

(604) Alphabet must check whether at least 1,000 (r) signed-in end users have issued a query with the same metadata attribute values for inferred language, location information, and device type. If such condition is not met, Alphabet must generalise the location to country level. If the r-threshold is still not met, meaning that fewer than 1,000 (r) end users submitted queries with the same inferred language and device type in a given country, Alphabet must remove the query and its corresponding results and metadata from the Search Data.

(605) Within each metadata group, click back time and interaction durations (e.g., hovering and viewing) must be binned into time intervals expressed in milliseconds and corresponding to the: 20th, 40th, 60th, and 80th percentile of their respective duration distributions within the metadata group.

(606) **Mini-sessionisation**: Alphabet must group records by ordering all records from the same end user chronologically and adding each search record to the previous group if the following conditions are met:

(a) The current search record was generated by one of the following ways:

(1) The user clicked on a query modifier (e.g., "*Did you mean…*" spelling suggestions, autocomplete suggestions, query suggestions, query shortcut chips, entity results, etc.) in the previous record's SERP.

(2) The user entered a new query into the search box on the previous record's SERP, and the previous record's query text is a substring of the current search record's query text.

The maximum length of a mini-session must be three queries, and a query can only be part of one mini-session (i.e., mini sessions must not overlap). Clicked modifiers from the last query in a mini-session must be suppressed.

(607) Alphabet must tag each search record associated with a group with the same unique random identifier and provide them in chronological order. The location and device metadata of all records in a mini-session are overridden with the location and device metadata of the last record of this mini-session.

---

945 See https://ec.europa.eu/eurostat/web/nuts, Doc ID […], (last accessed on 29 June 2026).

(608) Alphabet must include all other data (as defined in section 4.3.2) unaltered, without applying any additional measures.

(609) Within the time limit set out in section 4.6.4, Alphabet must communicate for the Commission's review:

(a) Which personal data detectors and which entity types Alphabet intends to use to recognise entities as part of query suppression, including the parameters such as the likelihood threshold (confidence) of each detector. Alphabet must explain why it has identified its proposal as the best performing option and why alternatives identified are less suitable.

(b) A list of result types that link to Google services which directly include personal information saved in an end user Google account (e.g., Google Maps results with directions to or from home) or the end user's exact location (e.g., Google Maps result with directions) which must be suppressed (see recital (596)(j)).

(c) The computing resource cost for each of the steps that are part of the technical anonymisation measures, including a detailed explanation of what factors drive the computing cost of each step.

(610) If Alphabet includes any attributes in the dataset that are not explicitly mentioned in section 4.3.2, it must determine whether any anonymisation measures are required in relation to that attribute. If so, Alphabet must propose to the Commission an appropriate anonymisation measure in relation to that attribute, which does not unnecessarily degrade the quality or usefulness of the data. As part of its proposal, Alphabet must provide a quantitative estimate of the proportion of data altered and suppressed by the proposed measure.

(611) Alphabet must provide to eligible recipients the following information in relation to the technical anonymisation measures on a quarterly basis:

(a) Which personal data detectors and which entity types Alphabet used to recognise entities as part of query suppression, including the parameters used such as the likelihood threshold (confidence) of each detector and detection performance statistics. Alphabet must use publicly available personal data detectors (e.g., Google Sensitive Data Protection).

(b) The proportion of unique queries and query volume suppressed and altered for each anonymisation measure and each personal data detector separately, computed over the full quarter.

(612) Alphabet must update the Commission on relevant technological developments.

4.4.4.1.2. The Commission's assessment

(613) The Commission's technical measures have been designed to enable the sharing of search data at record level daily, while altering this record level search data through suppressing identifying data points entirely, tailored and calibrated query suppression, metadata generalisation and mini-sessionisation measures which, together, effectively mitigate the risks of end users' re-identification to a residual level[946] (see recital (618)), while preserving the most quality and usefulness of the data for third-party OSEs in line with the legal framework set out in section 4.4.1.

946 In this Section and more generally in the Decision, the Commission uses the term "residual level" to designate the level of end users' re-identification risk that remains after application of technical measures in accordance with the Commission's risk assessment explained in recital (618).

(614) For the purpose of elaborating an alternative anonymisation method, the Commission has commissioned an expert report from a recognised expert in the field of anonymisation (the "**Expert Report on Anonymisation**")[947] and relied on its own in-house expertise. The Commission has also commissioned two recognised experts in the fields of anonymisation and adversarial privacy assessments to conduct data testing (see section 4.4.4.1.2.1.7 below). Additionally, the Commission has considered alternative anonymisation approaches submitted by third parties,[948] feedback from the public consultation (see recital (629) et seq. below) and information provided by Alphabet in various meetings and responses to the Commission's requests for information.

(615) This section demonstrates that, together, the Commission's technical anonymisation measures (i) reduce the risk of re-identification of end users to residual level (see section 4.4.4.1.2.1), and (ii) maintain a higher level of data quality and usefulness than Alphabet's current anonymisation approach or Alphabet's alternative anonymisation approach (see section 4.4.4.1.2.2).

4.4.4.1.2.1. The Commission's technical measures reduce risk of re-identification of end users to residual level

(616) This section demonstrates that the technical measures, taken together, reduce the risk of re-identification of end users to residual level. The section first sets out the Commission's approach to the assessment of main re-identification risks - including singling out, inference and linking risks – and then explains how each of the Commission's technical measures contributes to their mitigation.

4.4.4.1.2.1.1. Risk assessment

(617) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share ranking, query, click and view data. Under the regulatory framework of this provision, data sharing has a clearly defined scope, which only includes gatekeepers and third-party undertakings providing online search engines and their subcontractors acting as processors.[949] Unlike a public data release, this sharing is limited to a specific set of potential beneficiaries, who are subject to eligibility criteria (see section 4.2) and to an independent verification mechanism (see section 4.4.4.2.4).

(618) As set out in recitals (553) and (593), the Commission's technical measures are indispensable and play a prominent role in reducing the risk of re-identification to an insignificant level.[950] More specifically, the Commission's technical measures reduce the overall re-identification risk to a residual level without substantially degrading the data quality and usefulness and the contractual measures further mitigate that residual risk to an insignificant level.[951]

---

947 Expert report on Anonymising search data to comply with DMA Article 6(11) ("Expert Report on Anonymisation"), Doc ID […].

948 For instance, proposed approaches by [market participant], Doc ID […], and [market participant], Doc ID […].

949 Joint Guidelines, Doc ID […], paragraph 187.

950 According to the Joint Guidelines, the use of appropriate technical measures that result in the alteration of the data to be provided is "indispensable", as anonymisation cannot be achieved through contractual measures only (Joint Guidelines, Doc ID 1[…], paragraph 181). In addition, in line with the EDPB comments on the proposed measures of 5 May 2026, paragraph 9 (Doc ID […]), the Commission considers that the specified technical measures play an essential role, which is prominent, in making the risk of re-identification insignificant.

951 Joint Guidelines, Doc ID […], paragraph 181.

(619) In the specific context of data sharing under Article 6(11) of Regulation (EU) 2022/1925, the Commission assesses risks in light of the framework proposed in the Expert Report on Anonymisation according to which risks are considered beyond residual level after application of technical measures if they meet any of the following criteria:

(a) An adversarial entity can choose a specific individual and, with significant probability, retrieve some of their search records with high certainty.

(b) An adversarial entity can choose a random search record and, with significant probability, re-identify the end user with high certainty.

(c) An adversarial entity can perform attacks that re-identify a large number of end users with high certainty and with reasonably simple methods.[952]

(620) That risk framework, which is applied for the Commission's assessment of whether technical measures reduce re-identification risks to a residual level, takes into account objective factors, namely the efforts required in terms of time, cost, manpower and available technology to re-identify end users under foreseeable circumstances,[953] in particular in the context of both targeted attacks (first criterion)[954] and untargeted attacks (second and third criteria)[955] by any adversarial entity (whether the third-party OSE, a malicious employee or an unintended third party as explained below in recital (621)), as well as the potential information gain from performing the attack (i.e., what the attacker might learn that was previously unknown about the re-identified individual and the confidence with which they can make this inference).

(621) The Commission's technical measures are based on a thorough assessment of the risks of end users' re-identification, namely the inference, linking and singling out risks, which are recognised as essential to anonymisation,[956] and an assessment of the overall risk of re-identification taking into account these risks. Contrary to Alphabet's approach (see recital (574)), the Commission's assessment considers likely attack models and adversaries under the specific sharing context of Article 6(11) of Regulation (EU) 2022/1925 and maps them against the potential attacks and residual risk criteria.

(622) Taking into account the specific circumstances of the case at hand, namely the disclosure of record-level search data and the requirement to ensure anonymisation of end users' personal data (and not of any individual; see recital (551)), the Commission has taken into account the risks of end users' re-identification by reference to identifiable categories of potential attacks as follows:

(a) **Inference risks:** Inference refers to the possibility to deduce, with significant probability, the value of a previously unknown attribute from the values of a

952 Expert Report on Anonymisation, Doc ID […], section 4.5.

953 Recital 26 of Regulation (EU) 2016/679 and Judgment of the Court of Justice of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016-779, paragraph 46.

954 In the present context, a targeted attack as set out in the first criterion of recital (619) consists in an attempt to re-identify a specific end user's search records from the Search Dataset, relying for example on information that the attacker already knows about that specific end user.

955 In the present context, untargeted attacks as set out in the second and third criteria of recital (619) consist in attempts to re-identify randomly one or more end users' search records from the Search Dataset.

956 See also Alphabet's Expert Opinion: The Anonymisation Requirement under Article 6(11) of the DMA in the context of the GDPR of 28 November 2024, Doc ID […], paragraph 21 and subsequent Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], page 13.

set of other already known attributes from identifiable end users. This risk may materialise if an attacker, e.g., an indiscreet employee, accesses the Search Data and attempts to re-identify specific records or to find the record of a specific end user by using direct identifiers, and infers new information about the identified end users issuing a query (e.g., their demographics) or retrieves a shared secret (e.g., a private zoom link with a password).[957] The same situation may occur in the unlikely event where an external attacker would access a meaningful portion of the Search Data through a data breach (which presupposes that the attacker will have successfully bypassed the high level of security protection required to access the Search Data as specified in section 4.4.4.2.3) and attempts to re-identify and infer new information about end users,[958] for example to harm them and the reputation of the Search Data recipient, or extract commercial value out of the new information.

(b) **Linking risks**: Linking refers to the possibility to correlate or directly connect records of an end user or group of end users between different sources. This risk may materialise if an attacker, e.g., an internal business unit or an external attacker, seeks to derive commercial value or to harm an end user by linking Search Data records to other sources of information where the end user may appear, like auxiliary datasets[959] or contextual knowledge known by an indiscreet employee about an end user. For example, an attacker may attempt to profile an individual by linking Search Data with third-party cookies from an ads network, social media profiles, or accessible medical records. Besides URLs, these attackers primarily rely on metadata attributes to correlate records and reconstruct end user level patterns with third-party tracking cookies, which may be used to harm the end user.[960] The risk and practical feasibility of linking attacks is highly dependent on the availability of auxiliary data, which varies widely depending on whether a given hypothetical attacker has access to relevant proprietary data and on the breadth and quality of this data.[961]

(c) **Singling out risks**: Singling out refers to the possibility to isolate some or all records that identify an end user in the Search Data.[962] This risk materialises if an attacker, either an indiscreet employee or an external entity, tries to isolate and identify Search Data about a specific end user leveraging direct or indirect identifiers (e.g., a passport number or location information) or shared secrets (e.g., usernames and passwords) contained in the query text and metadata. These attackers may single out end users as a first step to launch a re-identification attack. However, singling out records, although a potential means towards re-identification[963], does not necessarily constitute a successful re-identification attack. To achieve successful re-identification, it is essential to not only isolate specific records but also to reliably link that information to a particular individual.

---

957 Expert Report on Anonymisation, Doc ID […], paragraph 359.

958 Expert Report on Anonymisation, Doc ID […], paragraph 365.

959 Expert Report on Anonymisation, Doc ID […], paragraph 97.

960 Expert Report on Anonymisation, Doc ID […], paragraph 97.

961 Expert Report on Anonymisation, Doc ID […], paragraph 351.

962 In the present context, singling out requires the ability to isolate some or all records relating to a specific end user in a manner that distinguishes those records from records relating to other end users. The mere fact that Search Data is organised per record and that each record obviously relate to an end user does not suffice to distinguish a particular end user within the dataset. Interpreting singling out otherwise would lead to the unreasonable conclusion that any record-level dataset inherently enables singling out.

963 Recital 26 of Regulation (EU) 2016/679.

(623) This risk categorisation framework has been considered by Alphabet as well in the course of designing its current anonymisation approach.[964] However, Alphabet's overall approach to risk assessment in relation to the Google Search Data does not correctly reflect the personal data scope of the anonymisation requirement in Article 6(11) of Regulation (EU) 2022/1925 (see section 4.4.1). Alphabet's risk assessment is not confined to risks relating to the re-identification of end users. Instead, its risk assessment also encompasses privacy risks relating to other identifiable individuals whose data may appear in search queries. This is also the approach that Alphabet follows in its expert report, which considers both the end user inputting personal data about themselves and about other individuals,[965] as well as in its expert legal opinions on anonymisation, which fail to take this distinction into account in their legal analysis.[966]

(624) For each of the possible attacks, the Commission considers that the extent of the information that an attacker is expected to obtain from a successful attack (i.e. "information gain") is also a relevant and objective factor, alongside other factors, for the assessment of whether technical measures reduce re-identification risks to a residual level in the specific context of Article 6(11) of Regulation (EU) 2022/1925. On the one hand, the expected information gain informs the assessment of the consequences of a successful attack. Where a successful attack attributes a single search record to an identified individual but reveals only limited additional information, the privacy risk associated with the attack is correspondingly limited. For instance, even if using personal knowledge about a specific person to re-identify that person's records may in some cases be possible, this is unlikely to lead to additional information gain (e.g., if an attacker knows that an end user is currently looking to buy a 2-room apartment in a given neighbourhood, the attacker may try to find queries about this exact topic. However, this does not teach the attacker anything new about that end user). Since queries are not sessionised, attributing a single record to a specific end user based on auxiliary personal knowledge about that end user is unlikely to convey material additional information to the information that the attacker already knew and used to attribute that specific record to the identified end user. It must be noted that to find a specific record in the Search Data, an attacker needs to have knowledge about e.g., the query text and key metadata attributes, like the device type used to issue that query and likely location of the end user when he/she issued that query. It follows that even in the circumstances where an attacker knows that someone searched for a specific query and finds this query in the dataset associated with the expected metadata attribute (e.g. device type and location), the attacker would not learn material additional information about this person from the record in question. On the other hand, the expected information gain also affects the practical likelihood that such an attack would be undertaken in the first place. Where a successful attack is expected to provide only limited additional information, the

964 Alphabet's internal report "Search Metadata Privacy for DMA 6(11)", Section "Regulatory Context", Doc ID […], GOOGLE-DMA6(11)-USPriv-00000007, pages 5 and 6. It has also been considered by [market participant] in its proposed anonymisation approach, see [market participant]'s report "Anonymizing search click-and-query data under the DMA", Doc ID […], page 3, where [market participant] uses the three privacy risks of inference, linkability, and singling-out for its anonymity assessment.

965 Alphabet's study "Privacy Expert Report on DMA Art. 6(11) Google Search Data Sharing", paragraphs 56 and 57, authored by Dr. Chris Culnane & Prof. Ben Rubinstein, Doc ID […].

966 Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], and initial Alphabet's Expert Opinion: The Anonymisation Requirement under Article 6(11) of the DMA in the context of the GDPR of 18 November 2024, Doc ID […].

practical likelihood that the time, cost, manpower and available technology required to carry out that attack would be deployed, in particular at scale, is correspondingly reduced.

(625) Alphabet argues that with advanced AI, the risk of re-identification at scale has increased, and presents a recent academic paper in support of this argument.[967] However, the scenarios covered in this paper are substantially different from Search Data sharing under Article 6(11) of Regulation (EU) 2022/1925. The paper uses AI to re-identify pseudonymised Hacker News users based on their comments and stories which are summarised in a structured profile. As an additional scenario, the paper uses Anthropic Interview transcripts to re-identify pseudonymised interview participants. Both types of data are structured per individual and are vastly richer than the Search Data (e.g., the partially redacted interview transcripts from Anthropic consisted of lengthy conversations between each participant and an AI chatbot). They therefore contain much more information and cues that can be used to re-identify users than the Search Data, which consists of short individual queries that are not pseudonymised (i.e., the contributions of a given end user are not associated with the same identifier), and re-sessionisation is complex, error-prone, and involves uncertainty (see section 4.4.4.1.2.1.7). Additionally, the technical measures applied to Search Data go well beyond the pseudonymisation used for the experiments. The academic paper's findings can therefore not be generalised to the Search Data shared under Article 6(11) of Regulation (EU) 2022/1925. Additionally, relying on an LLM to launch a re-identification attack at scale across billions of search records would be expensive and require significant manual effort to validate the large language model's output. As attackers do not have the ground truth available, this further limits the certainty an attacker could get that their results are correct. These factors undermine the effectiveness of an LLM-supported attack.

(626) Alphabet argues that the Commission's anonymisation measures are *ad hoc* and unprincipled. As will be set out below, this is not the case. The Commission's measures are based on one of the most established and broadly-accepted anonymisation techniques: they remove direct identifiers and apply *k*-anonymity to the relevant metadata. Additionally, the Commission's anonymisation measures follow from clear attack modelling that takes into account the data sharing context of Article 6(11) of Regulation (EU) 2022/1925 – in contrast to Alphabet's approach. Instead, the main source of disagreement between Alphabet and the Commission is which data attributes should be considered as quasi-identifiers. Alphabet adopts an unduly expansive conception in this regard and considers that the query text is a quasi-identifier that should be subject to *k*-anonymity. As is explained below, the query text need not be considered a quasi-identifier in the data sharing context of Article 6(11) of Regulation (EU) 2022/1925.

(627) Alphabet further argues that the Commission would have no benchmark or evidence to conclude that the reviewed technical measures reduce re-identification risks to an acceptable level.[968] Contrary to Alphabet's claim, the risk framework presented in recitals (619) and (620) builds upon the objective factors stemming from Regulation (EU) 2016/679 and relevant case law[969] and provides clear reference criteria against which end users' re-identifiability is assessed. More specifically, the framework

---

967 "Large-scale online deanonymization with LLM" by S. Lermen, D. Paleka, et al. See https://arxiv.org/abs/2602.16800, Doc ID […], last accessed on 11 March 2026.

968 Alphabet's response to the Revised Measures,15 June 2026, Doc ID […], paragraphs 9-23.

969 Recital 26 of Regulation (EU) 2016/679. See also Judgment of the Court of Justice of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016-779, paragraph 46.

evaluates whether a foreseeable attacker could successfully re-identify end users through targeted attacks against a known end user, through attacks starting from an arbitrary record in the dataset, or through scalable attacks affecting a significant number of end users. Each attack scenario therefore embeds considerations of the likelihood of successful re-identification, the certainty of the resulting identification, the resources required to perform the attack, including the time, cost, manpower and technology available to a reasonably foreseeable attacker, the quantity and quality of auxiliary information required to achieve the attack and the information gain obtained from an attack.

(628) It follows that these attack scenarios, together with the associated criteria set out in recital (619), provide concrete reference points for determining whether the remaining re-identification risk after application of the technical measures exceeds a residual level as defined in the case at hand for an effective implementation of Article 6(11) of Regulation (EU) 2022/1925. Contrary to Alphabet's claim,[970] the respective contribution of technical measures and contractual measures to ensure end users' anonymisation in the context of Article 6(11) of Regulation (EU) 2022/1925 is not left open: while the technical measures are indispensable and play a prominent role in reducing the risk of re-identification to a residual level without substantially degrading the data quality and usefulness of the Search Data for its legitimate use by eligible third-party OSEs (see section 4.4.1 and recital (618)), the contractual measures set out in section 4.4.4.2 further mitigate that residual risk to an insignificant level. The Commission does not consider it necessary to set more specific criteria than those already provided in the risk framework outlined in recitals (619) and (621) for the assessment of end users' re-identifiability after application of technical measures since the contractual measures comprehensively complement the technical measures to ensure, altogether, end users' anonymisation in a way that enables an effective implementation of Article 6(11) of Regulation (EU) 2022/1925.

(629) Alphabet purports that the results of the public consultation are highly critical of the Commission's proposed technical measures.[971] The Commission's public consultation as well as Alphabet's widespread effort to influence the responses, are described above in the section 2.2.4.

(630) Particularly on anonymisation, Alphabet has made far-reaching misrepresentations of the Preliminary Findings in its outreach to participants. When reaching out to participants, and in some cases providing compensation to contribute to the public consultation, Alphabet shared a pamphlet with statements on the proposed anonymisation measures. This pamphlet provides a deeply distorted view of the anonymisation measures proposed in the Preliminary Findings:

(a) The pamphlet makes no mention of the regulatory context in which the data is shared (with eligible beneficiaries only), the scope of the anonymisation requirement (end users issuing the query only) or the rigorous contractual measures that complement the technical measures to ensure end users' anonymisation.

---

970 Alphabet's response to the Revised Measures, Doc ID […], paragraphs 9-15.

971 The Commission notes that the public consultation is intended to collect input on the measures proposed in the Preliminary Findings, not on Article 6(11) of Regulation (EU) 2022/1925 itself. Shortly after a media campaign by Alphabet in which it claimed that the measures put personal data at risk, the Commission received several very brief contributions which did not engage with the measures proposed in the Preliminary Findings, but object to the transfer of data altogether, or were under the impression that the Commission would gain access to search data. Alphabet portrays these contributions as critical of the Commission's findings.

(b) The pamphlet asserts that the Search Data will be released "in the wild" rather than a controlled release to eligible beneficiaries.

(c) The pamphlet refers to the anonymisation measures as "name-scrubbing", which wholly misrepresents the measures.

(d) The pamphlet presents examples of sensitive queries which the proposed anonymisation measures would suppress, for instance:

(1) "*Registration no. 129042025, DOB 22/08/2025 name Elena Schmidt, parents Lukas Schmidt, Sophie Weber-Schmidt…*". This query has 106 characters, while the Commission's length threshold stands at approximately [50-75] characters.

(2) "*Revolut bank limited iban: be47 1260 0813 8640 21 name: matthieu janssens*". This IBAN number should be recognised by the personal data detector and suppressed by the entity threshold.

(631) The Commission has carefully reviewed and considered all contributions received in response to the public consultation. Where appropriate, the measures in the present Decision reflect changes to the measures and clarifications that address public consultation input. For example, some contributions indicated that it was unclear whether metadata generalisation covers the query text and what is the exact scope of mini-sessions. The present Decision includes clarifications in these areas. The measures were also amended in response to comments raised in the public consultation. For instance, the metadata threshold has been increased, interaction data has been further coarsened and the measures now provide transparency regarding the implementation of personal data detectors in the context of the entity threshold. Where comments propose changes that are not appropriate, the Commission did not take them on board. For example, some respondents called for extremely granular location data. Other respondents called for making the Search Data available in an environment provided by Alphabet. However, the Commission's experience with accessing data in this way (see section 4.4.4.1.2.1.7) shows that this is not workable for recipients.

(632) Alphabet purports that in previous academic work[972] by Yves-Alexandre de Montjoye et al.,[973] singling out was presented to amount to re-identification. This is incorrect. Alphabet misrepresents the findings of the paper, which does not mention "singling out" even once. The paper covers a situation that is entirely distinct from the data sharing context under Article 6(11) of Regulation (EU) 2022/1925:

(a) The paper considers a dataset with pseudonymised data, which covers three months of credit card transactions organised by individual. This is a stark difference with the Search Dataset, which contains loose queries that cannot be readily attributed to the same individual.

(b) The paper covers a very specific attack model on this credit card dataset: a targeted attack where an attacker knows the target in the dataset, collects a handful of pieces of information about the target (e.g., day and shop where a credit card was used, approximate amount of the transactions for strong

---

[972] de Montjoye, Y., et al., *Unique in the shopping mall: On the reidentifiability of credit card metadata*, Science 347 (2015), Doc ID […].

[973] Yves-Alexandre de Montjoye is Chief Technology Officer in the Commission's Directorate General for Competition since February 2026. In this capacity, he is closely involved in the work of the Commission on the elaboration of an alternative anonymization method for the purpose of the present Decision.

attackers) and then uses this information to identify the target and uncover three months of credit card transactions.[974] In this context, the paper uses unicity to quantify risk: how often is a handful of randomly chosen datapoints sufficient to uniquely identify an individual.

(c) The crux of the attack presented in the paper is that an attacker may reasonably know a few shops where an individual made purchases over a few days (e.g., by observing shopping bags). This may uniquely identify the individual in the data, and the pseudonymous nature of the data then allows the attacker to learn all other purchases the individual made over the time period covered by the dataset.

(d) This attack does not generalise to the Search Data. First, the Search Data consists of loose queries, meaning that re-identifying the user behind a single query does not reveal their entire search history. Second, unlike information on purchases, it is not a reasonable assumption that an attacker knows the *exact* query issued by an end user on a specific day, location and device type. Third, even if this information were known to an attacker (*quod non*), the information gain is minimal, as it would only allow re-identification of a single record, of which the attacker already knew. Indeed, as the dataset consists of loose queries, one re-identified query does not put other queries by the same user at risk, further mitigating privacy risk of this hypothetical attack.

(633) Alphabet and some of the public consultation contributions have drawn comparisons between the measures proposed in the Preliminary Findings and the 2006 AOL search log release, which led to re-identification of users. However, such comparisons are misplaced as there are fundamental material differences between the two data sharing scenarios. First, the AOL case concerned a public data release, whereas data sharing under the present Decision concerns a controlled release to a limited number of eligible beneficiaries, subject to strict contractual conditions. Second, the AOL dataset was pseudonymised, meaning that full search histories were attributable to the same user through a numeric ID. By contrast, the Search Dataset consists of loose queries that are not readily attributable to the same user. Third, beyond pseudonymisation, no further protections seem to have been applied to the AOL data. By contrast, the Search Data has extensive additional protections applied to it, such as suppression of sensitive attributes, query suppression and metadata generalisation.

(634) As will be demonstrated below, the Commission's technical measures, taken together, mitigate the risk of end user re-identification to a residual level, considering singling out, inference and linking risks, and in accordance with the risk assessment described in this section.

4.4.4.1.2.1.2. Attribute suppression

(635) The technical anonymisation measures require Alphabet to remove certain attributes from the Search Data altogether. The attribute suppression step removes any end user identifier accompanying the search record, such as account identifiers (e.g., account IDs, usernames), other associated direct identifiers (e.g., IP addresses, device IDs), and other attributes containing potentially unique values such as the query's precise timestamp (see recital (596)). This first measure turns the dataset from data that is organised by end user, as available for Alphabet's use to improve Google Search, to a large "haystack" of queries that are not attributed to a given end user. This means

974 Alphabet has not shown a single successful example of such a targeted attack on the Search Data.

that the queries are loose datapoints provided in random order, without information on the end user that submitted the query or that two queries originate from the same end user. Attribute suppression ensures a strong baseline protection against the re-identification of end users and strongly limits the information gain of any successful re-identification. Already based on this measure, any attacker would have to put in significant effort to re-identify users.

(636) Third parties confirm that removal of these identifiers already greatly contributes to mitigating risks of direct identification from the Search Data. For instance, one third party "[...] *believes that if identifiers are removed, and only clicks, query, ranking, and view data are shared in a non-sessionized fashion, the risk of identification or re-identification, using other data sources available, is extremely small.*"[975] However, the Commission's technical measures go well beyond removing direct identifiers by applying a range of additional measures as described in the next sections.

(637) In addition to direct identifiers, the Commission has reviewed the full scope of search data to be shared under Article 6(11) of Regulation (EU) 2022/1925 considering the results of Alphabet's red team testing of the Commission's preliminary technical Measures and comments from the public consultation. Wherever attributes pose a re-identification risk that cannot effectively be mitigated to a residual level by the remaining technical measures, such attributes are removed, namely:

(a) **Timestamp.** The timestamp of a query can pose re-identification risks, as it may help attackers sequence queries (and subsequently turn them into sessions). The precise timestamp that Alphabet collects is therefore removed from the Search Dataset. The dataset still contains implicit information about timestamps due to the daily release frequency. This frequency means that recipients know only the day on which a query took place.[976]

(b) **Information about the height and size of modules and results; the distance from each module or result to the top of the SERP; and the share of the user's viewport that each module or result occupies.** Each of these pieces of information allows recipients to infer the size of the end user's screen. This information implicitly provides far more granular information on device type than that shared in the device type attribute, which only distinguishes between mobile, tablet and desktop. Such granular information could be used to link different queries together and poses practical challenges in terms of generalisation.

(c) **Access point and input format.** Rare access points and input formats may be used to attribute queries within a metadata bucket to the same user and could in that way contribute to a re-sessionisation attack.[977] Moreover, beneficiaries did not generally consider these attributes particularly important to the quality and usefulness of the data.

---

975 Agreed minutes of meeting with [market participant]on 13 June 2024, Doc ID […].

976 Release frequency involves a trade-off with metadata generalisation: as the metadata generalisation step generalises metadata attributes to achieve indistinguishability among end users, more frequent releases mean that metadata will be provided in a more generalised way. Expert Report on Anonymisation, Doc ID […], paragraph 166.

977 Alphabet raises this risk in its response to the Preliminary Findings, Doc ID […], paragraphs 212 and 213a. Suppression of these fields fully addresses this risk.

(d) **Ad URLs.** Ads are often personalised to the user. Therefore, Alphabet argues they can be used to identify sessions within a metadata bucket.[978] For example, the top-level domain can indicate a country and language other than the country from which the query originated or the query language. This may allow linking queries within a metadata bucket. Removing ad URLs effectively mitigates these risks.[979]

(e) **Advanced filters applied to a query.** Advanced filters can be applied to a query to narrow the results that Google Search returns. For instance, end users can set filters to specific file types. Alphabet argues that such filters are rare and persist across queries, allowing to attribute queries with the same filter to the same end user.[980] Removing information on such filters mitigates this risk effectively.

(f) **Google services which directly include personal information from a user account or the end user's exact location.** Alphabet argues that some result URLs reflect information that an end user chose to save to their Google account, such as home address.[981] As an example, Alphabet presented the scenario where a query such as "*directions from home to <place>*" may reveal the end user's home address. Similar risks arise from Google Maps results that provide directions from an end user's exact location. Alphabet has not identified additional examples. Removing result URLs that directly reveal such information effectively mitigates this risk. In case there are other URLs than Google Maps URLs that present similar risk, such as Alphabet service Waze, Alphabet must submit these risk types to the Commission for approval, to ensure that result URLs are not removed unnecessarily. For the avoidance of doubt, third-party URLs that may have received a higher ranking on the results page due to personalisation, or results that were influenced by an end user's location (e.g., nearby restaurants) must not be suppressed, as this information is difficult to identify and link together with high certainty.

Alphabet argues that the measure requiring suppression of such result URLs is ill-specified, hard to understand, and would be difficult to reliably implement in practice.[982] This is not the case. The measures provide that Alphabet must provide a list of such results to the Commission for review. This process allows iteration on the list, and clarification of the result URLs to be suppressed. Therefore, any concerns Alphabet may have about its understanding of the measure can be resolved through this process. Alphabet also suggests that as an alternative measure, *all* personalised results should be suppressed. However, Alphabet provides no reasoning for this position and has not shown persuasive evidence of re-identification risk stemming from indirect personalisation (e.g., difference in result ranking based on age of the end user).

(g) **Follow-up queries in AI Mode.** The Search Dataset must include queries entered by the end user in AI Mode. However, it must not include the

978 Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], Section V and Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 100d, 201-204.

979 This adjustment was also proposed by Alphabet in its alternative anonymisation proposal of 19 May 2026.

980 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 73-91.

981 Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], Section VI

982 Alphabet's response to the Revised Measures, dated 15 June 2026, Doc ID […] paragraphs 106-108. Alphabet also argues that there is no such thing as a "Google Search account". For clarity, this reference has been changed to "Google account".

subsequent queries after the first query within the same search session in AI Mode. This is because these queries are more likely to be of "conversational" nature and thus closely connected, which may present a higher risk of re-sessionisation and ultimately of re-identification. AI Mode is also a new service whose characteristics and use are just starting to be observed. In light of this novelty and on a cautionary basis, it is therefore appropriate to exclude follow-up queries within the same search session in AI Mode.

(h) **Queries in the form of images.** Google Search allows users to enter an image as a query. Images may be rich with personal information (e.g., faces) and anonymising such input images poses practical challenges. However, that does not prevent the possibility of sharing the data associated with such queries (click, view and ranking data). Image queries must therefore be removed and replaced by a placeholder query indicating that the original query was an image (e.g., a placeholder saying {IMAGE}). For queries that combine images and text, only the image must be replaced with a placeholder query and the text must not be suppressed.

(638) Removing attributes such as direct identifiers is effective in reducing the overall risk of re-identification, and more particularly the risk that singling out could lead to re-identification. As lined out in the previous recital, several of the removed attributes additionally reduce the risk of successful attacks based on linking and inference. The risk of re-sessionisation as a step towards re-identification – i.e., the possibility to identify several distinct queries belonging to a given end user despite the removal of any end user identifier accompanying the search record – is addressed in the below recital (754) to (758).

4.4.4.1.2.1.3. Query suppression

(639) The Commission's technical measures require Alphabet to suppress queries containing rare entities as well as long queries. These steps serve to remove queries that contain likely unique identifiers (e.g., social service numbers or other identification numbers) and other secrets (e.g., bank account numbers) that could allow end-user re-identification.

(640) The Commission's query suppression method consists of two thresholds. The first one is an entity-based threshold that suppresses queries containing entities that appear less than 50 (w) times across the past 13 months of EEA data. Entities that meet this condition are added to an allow list for five years, this is similar to the allow list in Alphabet's anonymisation method (see recital (561)). It also applies a threshold on overall query length that removes all queries above a length that is calibrated to each inferred language, as different languages have different information densities.

Entity-based threshold

(641) Beyond Google Account end-user identifiers and other directly identifying information from the search records, like IP addresses (which are removed in the attribute removal step), other likely unique identifiers and secrets that allow direct end user re-identification are often specific words concerning their person, such as email addresses, package tracking numbers, passwords, and secret links that an end user may input in a query.[983] Full query suppression, including all metadata attached to the query, with a word-based threshold is effective to remove these potentially

983 Expert Report on Anonymisation, Doc ID […], paragraph 123.

sensitive words, as there are typically relatively few end users using these rare words in queries.

(642) Passwords, private links, social security numbers, among other likely unique identifiers, are present in many of the problematic queries highlighted by Alphabet's adversarial assessment of the potential privacy risks in the Search Data.[984] These types of search terms are unlikely to be searched by more than 50 signed-in users since words such as passwords are often unique to individuals (or at least they are unlikely to be shared by 50 signed-in users), meaning the EEA-based threshold removes information that could identify the end user issuing the query, undermining the attacker's ability to identify the end user and infer new information about them. For example, an end user may have accidentally entered their social service number in a query. Because this social service number is unique to the end user, it is unlikely to appear in queries of 50 different signed-in users, meaning that it would not meet the entity-based threshold. In cases where passwords pass the entity threshold, they are likely commonly used passwords (e.g., "password123") or consist of common words separated by spaces (sometimes called "passphrases"). This makes it difficult for an attacker to find such series of words in the data and reliably identify them as passwords. For example, an end user may have accidentally entered their password "*cassette lava baby*" in a query. As this password consists of common words, it is likely to pass the threshold. However, for the same reason, it is hard for an attacker to identify it as a password. Even when a password is recognisable as such, the attacker would additionally need to identify the account it belongs to and the associated log-in identifier.

(643) However, word-based thresholding may not filter out all such secrets, as some common types of secrets may contain whitespaces (e.g., bank account numbers and phone numbers). Using personal data detectors to recognise these entities addresses this issue. Additionally, entity recognition is also effective as a real-world risk mitigation measure as it limits the number of very rare names and addresses in the data which disclosure might lead to privacy harm even if they are not directly linked to end users (and therefore do not fall within the scope of the anonymisation requirement of Article 6(11) of Regulation (EU) 2022/1925, which covers end user personal data only). By applying entity recognition before applying the threshold, the threshold does not apply to each individual word (e.g., "John" and "Doe") but to the entity ("John Doe"). In this way, the query is only included if the entire entity passes the threshold, e.g., for addresses of known institutions that are searched for by many users.

(644) In summary, personal data detectors therefore enable the identification and suppression of rare entities, which include likely unique identifiers and secrets such as social service numbers and bank account numbers. As these types of secrets are known by few people, these queries are more likely to be made by the end user to which the personal data relates ("self-searches"). However, as set out in recital (750) below, the overall probability that a search is a self-search is low.

(645) By contrast, entities that appear above the defined frequency threshold are more likely to reflect queries carried out by multiple end users. In that case, a name or address included in a query often does not comprise end user's personal data. Names and addresses are typically known to a larger circle of individuals, including family, friends, acquaintances, employers, and others, compared to more sensitive

984 Alphabet's internal document "6(11): Anonymisation strategy and summary of insights", Annex 2 and 3, Doc ID 232, GOOGLE-DMA6(11)-USPriv-00000213.

information like passwords and secret links. As a result, many queries containing an end user's name and address may have been initiated by individuals other than the end user themselves, making it more challenging to reliably re-identify the end user based on names and addresses. In this regard, one third party explains: "*the data is already anonymous since there is no way to tie a query back to an individual. Even if a query contained a name, there is no way to know who searched it.*"[985]

(646) Entities that have been searched by more than 50 unique signed in users are unlikely to be secrets, as they are known and searched by a significant group of people.[986]

(647) Alphabet contests the effectiveness of the entity-based threshold based on the arguments set out below.

(648) Alphabet argues that controlling for rare words or entities is insufficient, because a combination of common words can be identifying. However, Alphabet's argument leans on the premise that the technical measures by themselves should reduce the re-identification risk to insignificant level, and that all personal data should be anonymised, rather than only end users' personal data.[987] However, this position runs afoul of recital 61 of Regulation (EU) 2022/1925. Recital 61 provides that what needs to be anonymised is the personal data of the end user generating the data, and not the personal data of other individuals that might be identifiable via the search data. Additionally, in the present context, contractual measures complement technical measures to mitigate the residual likelihood of reidentification that remains after application of the technical measures.

(649) Alphabet's examples of re-identification through combinations of common words in the query either remain hypothetical,[988] or do not demonstrate a re-identification risk beyond residual level. Alphabet has not shown an example of a targeted attack using combinations of common words in the query text, or indeed any examples of targeted attacks at all. Neither has Alphabet shown that the query text in a random search record allows reidentifying an individual with significant probability (see section 4.4.4.1.2.1.7). Finally, Alphabet has not performed attacks that allow identifying end users at scale from the query text (see section 4.4.4.1.2.1.7).

(650) In any event, the Commission's query suppression approach goes well beyond removing queries with words searched below a specific low number of times. The query suppression applies entity recognition, which is a combination of words, and applies the thresholds to entities rather than individual words.[989] There is a measure

---

985 [Market participant]'s Feedback on Compliance with Article 6(11), DMA (Click-and-Query Data) of 5 December 2023, Doc ID […].

986 The threshold is not particularly sensitive: doubling the threshold from 50 to 100 increases suppression from [10-20]% of unique queries to [10-20]% of unique queries when considering threshold level "possible" – a small increase of [0-10] percentage points. This means that a higher threshold does not meaningfully change suppression. See Alphabet's reply to RFI 16 of 22 May 2026, Doc ID […], question 1. Furthermore, while the context is different, the level of the threshold, w = 50, aligns with thresholds used by Alphabet in some of its public-facing products. For example, Ads Data Hub (see https://developers.google.com/ads-data-hub/guides/privacy-checks, Doc ID 1892, last accessed on 25 March 2026) and Privacy Sandbox (see https://privacysandbox.google.com/private-advertising/protected-audience-api/k-anonymity, Doc ID […], last accessed on 25 March 2026).

987 Joint Guidelines, Doc ID […], paragraph 181. The Joint Guidelines explicitly mention the query suppression approach applied by the Commission, saying that removing "queries with words searched below a specific low number of times" is an appropriate way to remove data liable to be used for identification (paragraph 188).

988 See Alphabet's response to the Preliminary Findings, Doc ID [...], Section II.B.

989 This is in line with the suggestion in the EDPB comments on the proposed measures of 5 May 2026, Doc ID […], paragraph 18. The length-based threshold is an additional measure that goes beyond individual word thresholding.

providing that Alphabet must provide detailed information on the entity detectors that it proposes to use. This is intended to enable the Commission to check that the detectors used are appropriate and that, beyond the examples specifically mentioned, all relevant entities / group of words are covered. The use of entity recognition has a material impact on suppression. Whereas applying a word-based threshold with threshold value 50 would remove fewer than [10-20]% of unique queries, applying the same threshold to entities removes [10-20]%[990] – an increase of [20-30]%. Additionally, the Commission's length threshold limits the length of shared queries to around [50-75] characters, or [number of words] words.[991] This further limits the amount of identifying information that could be shared through combinations of words.

(651) Alphabet further argues that names or addresses are not necessarily rare, and therefore not protected by the Commission's entity-based threshold.[992] However, this shows a misunderstanding of the purpose of the entity-based threshold. As set out in recital (642), the threshold is designed to remove secrets and likely unique identifiers such as passwords, private links and social security numbers. Names and addresses included in queries are in most cases not problematic: they are likely not self-searches, and even if they were, it is in most cases not possible to determine that. This means that names and addresses in queries that pass the entity-based thresholds are unlikely to allow an attacker to re-identify end users with high certainty (see also section 4.4.4.1.2.1.7 on the Commission's testing in this area).

(652) Alphabet's argument that the entity-based threshold provides uneven protection, for example for individuals that share their name with a celebrity,[993] is therefore misplaced. It is not the purpose of the entity-based thresholds to filter all names from the Search Data – its primary purpose is to remove secrets and likely unique identifiers, such as bank account numbers and social security numbers.[994]

(653) Alphabet argues that there is no data to support that self-searches are rare.[995] However, analysis of Alphabet's data (see also recital (750) et seq.) confirms that self-searches are rare compared to searches on others, making self-searches hard to detect. Considering a week of data, out of all users that searched for at least one name, [70-80]% of users searched for at least two different names. Even for those users that only searched for a single name within the week, it cannot be assumed that search is a self-search. Cursory inspection shows that these names often concern celebrities or brands. Even where the name is not a celebrity or a brand, it can be an acquaintance of the end user, rather than the end user themselves. This confirms that among searches for names, self-searches are the exception – not the rule.

---

990 Alphabet's response to RFI 12 of 11 May 2026, Doc ID […], question 4 and Alphabet's response to RFI 16 of 22 May 2026, Doc ID […], question 1.

991 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 169. This is the length limit for the English language.

992 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 158-161.

993 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 47-50.

994 The same is true for Alphabet's example concerning birthdates, put forward in annex 3 to its response to the Preliminary Findings, Doc ID […](paragraphs 54-58). It is not surprising that there will be dates in the data, and some of them might be the end user's date of birth. But just like names and addresses, they will generally not be an attribute that can be used for re-identification at scale and with high certainty, because the attacker typically cannot know whether the date is an end user's birthdate.

995 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 42-43. Alphabet's experts reference research from more than 20 years ago to support this argument. This is surprising, as Alphabet has the ground truth about the real names of its signed-in users. It is therefore trivial for Alphabet to check how often names in the data are self-searches.

(654) Hand-picked counter examples presented by Alphabet[996] do not contradict the conclusion that self-searches are rare. There may be cases, such as the one presented, where there are enough clues to make the determination that a search is a self-search with a reasonable level of confidence for someone performing an untargeted attack. However, this is not evidence that this can be done in an automated fashion with a reasonable level of confidence. This should therefore be considered a residual risk, in line with the criteria set out in recital (619).

(655) Alphabet further argues that an issue with entity detection is that quasi-identifiers can clash. Alphabet provides the example of a part number for an Opel Vivaro 2019 left front sliding door exterior handle, which has a similar pattern as an Irish passport number.[997] While such clashes can happen, this is unlikely to be an issue that occurs at large scale. Even where this is the case, it is likely not possible to say whether the number refers to a passport number or a part number without additional information. Alphabet's expert report confirms as much, indicating "*we have no way of telling, but it could be*".[998] Risk stemming from such clashes can therefore be considered residual.

(656) The Commission has considered approaches to query suppression suggested by third parties but has not adopted them for the reasons set out below.

(657) [market participant] proposed a word-based threshold with a suggested value of 10.[999] While the Commission finds that the word-thresholding method can constitute an effective and more proportionate component of its anonymisation method, the Commission proposes a stricter thresholding measure. First, the Commission proposes a threshold value five times larger than [market participant]'s (i.e., 50 instead of 10), second, the Commission's threshold considers entities instead of words, and third, the Commission adds an additional length-based threshold to remove more potentially sensitive queries that [market participant]'s approach would not capture.

(658) Some third parties have suggested a query suppression method based on filters that detect specific types of personal data, such as social security numbers and credit card numbers.[1000] However, they may suppress data that should not be suppressed, such as addresses and phone numbers of public entities that are frequently searched for. Therefore, the technical measures do not rely on filtering to remove end user personal data from queries. Using personal data detectors for entity recognition, as is proposed in the Commission's query suppression measure, does not suffer the same shortcoming. First, frequently searched names and addresses of public entities will still pass the entity-based threshold. Second, even if a certain rare identifier is not detected by the personal data detectors, it is still subject to the entity threshold, meaning it is not released if it was not searched for by at least 50 users.

(659) Another proposed approach by third parties is to redact words that do not pass the word-based threshold from the query text, instead of suppressing queries with rare

---

996 See e.g. annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 38-41.

997 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 51-53. Alphabet has not demonstrated that the hypothetical example in question, pr0007712, is indeed a valid passport number.

998 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 52.

999 [Market participant]'s report "Anonymizing search click-and-query data under the DMA", Doc ID […], page 10.

1000 [Market participant]'s report "Anonymizing search click-and-query data under the DMA", Doc ID […], page 8 and [market participant]proposal for Consistent Implementation of the article 6(11) Digital Markets Act among Gatekeepers dated 15 June 2023, Doc ID […].

words.[1001] However, it is unclear how much this would improve data quality and usefulness or what additional re-identification risk it creates. For example, it may be possible to infer the redacted words based on the result URLs. The technical measures therefore pursue the more conservative approach of suppressing queries, rather than redacting them.

(660) By removing secrets such as social security numbers through query suppression, the Commission mitigates the risk of singling out identifiable end users, as attackers can no longer reliably distinguish records based on such unique identifiers that an end user may have input in the query text. Furthermore, when attackers attempt to use a search record to infer new information about an individual, removing identifiers with query suppression mitigates the risk of inferring information about an identifiable end user. Additionally, the elimination of unique identifiers like phone numbers or social security numbers reduces the risk of linking, as attackers can no longer use these identifiers as keys to connect search records to other datasets, such as phone books or medical records, due to their suppression in the query text.

Length-based threshold

(661) The length threshold filters out the longest 5% of queries for each inferred language. Alphabet has argued that some queries are copy-pastes from private documents.[1002] Even in cases where such queries pass the entity-based threshold, such queries may contain re-identifiable information about end users. They are also less useful for third-party OSEs.[1003] The threshold on overall query length entirely removes these types of queries and is therefore effective to mitigate re-identification risks stemming from them. The length threshold is calibrated to each inferred language, as languages have different information densities, and therefore different average query lengths. In this way, queries enjoy similar protection regardless of language.

(662) Concerning the length-based threshold, Alphabet argues that personal data is not limited to long queries but can also appear in short queries and that the measures proposed in the Preliminary Findings leave these queries unprotected.[1004] This is incorrect. All queries are protected by the entity-based threshold and all other technical measures. The length-based threshold is an additional measure, to suppress the tail end of very long queries. As Alphabet's privacy expert concedes, "*the longer the query, the greater the possibility that it could contain user personal data.*"[1005] This is especially true as the length of a query can far exceed the truncated graphs included in the expert report. Suppressing this tail end of very long queries is not, as Alphabet contends, a concession or proof that the measures are "*ad hoc*". It is a prudent approach to suppress the tail end of very long queries, which pose a higher privacy and re-identification risk. Alphabet's back-of-the-envelope experiment confirms this: out of the 50 longest queries in its dataset, five were found to be likely to contain end user personal data. For a random sample of 50 shorter queries, only one was found to include personal data.[1006]

1001 See, for example, [market participant]'s submission of 17 January 2024, Doc ID […].

1002 Alphabet's study "Privacy Expert Report on DMA Art. 6(11) Google Search Data Sharing", paragraph 64, authored by Dr. Chris Culnane & Prof. Ben Rubinstein, Doc ID […].

1003 Expert Report on Anonymisation, Doc ID […], paragraph 137.

1004 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 168-171.

1005 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraph 70.

1006 Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraph 71. This experiment concerns query text before application of any anonymisation measures. Alphabet did not provide the personal data it claims to have found, so the Commission is not able to verify this example.

(663) Alphabet further argues that the Commission's threshold – which is updated weekly based on query length for that week – proposed in the Preliminary Findings is arbitrary and unprincipled, especially considering query length is growing.[1007] The measures in this Decision have set the length-based threshold at a fixed value, subject to monitoring by the Commission – meaning it is no longer relative. Additionally, setting a threshold at 95% of a distribution is not arbitrary, but is a common way in statistics to remove the tail of a distribution. Furthermore, the fact that a threshold has to be set at a certain plausible level within the Commission's discretion on technical assessments does not make that threshold arbitrary. As Alphabet's experts agree, the longer the query, the greater the possibility that it could contain end user personal data. The tail end of very long queries is therefore particularly risky, and putting a protection in place for these queries is a prudent step to take. That there is no predetermined boundary at which the threshold must be set does not take away the validity of the measure.

4.4.4.1.2.1.4. Metadata generalisation

Overview

(664) The Commission's technical measures require Alphabet to generalise metadata so that at least 1,000 signed-in end users writing queries in a given language and location and for a given device type are indistinguishable from each other. This achieves *k*-anonymity with k = 1,000, where 1,000 signed-in users is a lower bound and, in practice, the vast majority of users will be part of much larger buckets: 95% of unique signed-in users are in buckets that contain more than [>25,000] unique signed-in users,[1008] making any attempts to re-identify even less likely to succeed (see recital (671) below).

(665) Metadata may be used to re-identify end users and may pose a risk of re-sessionisation. For example, in sparsely populated areas, granular location information may be enough to identify which household a query came from. The inferred language of a query text may also be used to re-identify end users if an end user issues queries in a language that is rare in a given area. Furthermore, persistent rare metadata across queries could be used to re-sessionise queries even in the absence of direct identifiers (e.g., a series of queries issued from a very sparsely populated location with a rare device type). Metadata generalisation prevents such risks by ensuring that metadata is only disclosed at a granularity for which a certain number of users share the same combination of metadata attributes.

(666) Nevertheless, location is an important metadata attribute for the optimisation of search services (see recital (579)(c)). The metadata generalisation measures therefore generalise location to a larger area, ensuring that each record is provided with location information that is sufficiently coarse to prevent risk of re-identification. To ensure indistinguishability, the metadata generalisation also considers quasi-identifiers, namely the language of the query and the device type. Adding these fields to the metadata generalisation increases protection, as location will need to be more generalised to reach the threshold of 1,000 for all attributes.

(667) In short, the metadata generalisation considers whether at least 1,000 (r) signed-in end users have issued a query with the same metadata attribute values for inferred language, location information, and device type. If this condition is not met,

1007 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 164-168.

1008 Alphabet's response to RFI 12 dated 11 May 2026, Doc ID […], question 6.2. This assumes that every unique signed-in user appears in a single metadata bucket, and the metadata generalisation measures, which may combine or suppress buckets that do not meet the threshold, have not been applied.

Alphabet must generalise the location attribute to country level. The query is then shared with coarser location so that at least 1,000 signed-in end users issued queries with the same location, device type and inferred language. In the event that fewer than 1,000 signed-in end users have issued queries for a given inferred language on a given device type and in a given country, the query is removed from the dataset.

(668) The threshold value of 1,000 is in line with the metadata generalisation threshold proposed by Alphabet in its alternative proposal for anonymisation.[1009]

(669) Specifically concerning the generalisation of location data, the metadata generalisation outlined above generalises location data using Nomenclature of Territorial Units for Statistics (NUTS) geocode standard.[1010] The third level of this classification NUTS3, subdivides countries into smaller regions with populations that are typically between 150,000 and 800,000. This ensures that location data is provided at a level that is appropriate to the population density of a specific area. If fewer than 1,000 (r) users have issued queries within the NUTS3 region (e.g., because the query is issued in a rare foreign language), the location information is aggregated to country level. This is contrary to Alphabet's approach, which does not provide more granular location data than country-level, regardless of whether the country is large (e.g., Germany) or small (e.g., Cyprus).[1011] Alphabet's approach results in different privacy performance and data quality per country, as the area and number of users differs vastly per country. The NUTS-based approach in the technical measures does not suffer from this issue to the same extent, as location is provided by regions of similar population.

(670) Within each metadata group, interaction times and durations, such as click back time and hover duration, are coarsened. Alphabet argues that granular interaction data may be used to build a behavioural fingerprint that can be used to re-identify end users.[1012] However, interaction data is a noisy signal, not a fixed attribute. It can change between queries even if they originate from a single user, meaning that an attack based on these signals is non-trivial and uncertain. Coarsening interaction data into ranges based on percentiles of the time distributions therefore is a conservative measure to further mitigate such fingerprinting risk, as it reduces the amount of information available to an attacker which limits the ability to run behavioural profiling attacks. Applying the coarsening to the specific distribution of durations in a given metadata group ensures that each bin will have a similar and large number of queries in it. Applying the coarsening based on the global distribution could create a situation where a given metadata group only contains few queries that fall within a given bin. This is not the case when determining the distribution based on the metadata group, thereby ensuring that sufficient end users are in each of the bins.[1013]

(671) The metadata generalisation effectively thwarts an attacker attempting to leverage the metadata attributes of location, device type, and inferred language to single out users, as at least 1,000 users with identical metadata will be present in the dataset. In most cases, there will be far more than 1,000 users with shared metadata attributes. This is

---

1009 Alphabet's alternative anonymisation proposal of 19 May 2026, Doc ID […].

1010 https://ec.europa.eu/eurostat/web/nuts/overview, Doc ID […], (last accessed on 29 June 2026).

1011 By way of comparison, Germany has 400 NUTS3 regions, while Luxembourg only has one.

1012 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 205-211 and Annex 3 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraphs 102-104.

1013 This addresses Alphabet's argument that the coarsening of interaction data should take place on daily level. See Alphabet's response to the Revised Measures, dated 15 June 2026, Doc ID […], paragraph 60. By applying it to metadata groups, not only does the coarsening take place on daily level (given that is the frequency of the data release), it is also adjusted to the metadata group.

because NUTS3 regions are large and have a population that is typically between 150,000 and 800,000. Because of this, NUTS3 regions typically contain far more than 1,000 active users for the more common language in each region.[1014] The minimal bucket size of 1,000 should be considered a lower bound, which protects, for instance, users issuing queries in languages that are rare in a given region. The vast majority of users are in far bigger buckets: 95% of unique signed-in users are in buckets that contain more than [>25,000] unique signed-in users.[1015]

(672) Similarly, inferring information from generalised attributes becomes progressively harder. For example, if location has been generalised to a region containing several major cities, it becomes harder for the attacker to determine in which city may the end user live.

(673) The same is true for attackers attempting to perform a linking attack with external sources of information (e.g., another dataset or with personal knowledge about an end user, such as nationality and residency). The metadata generalisation coarsens location, device type, and language to ensure that at least 1,000 (*r*) end users share the same metadata values. This means that an attacker cannot link the external source of information to the Search Data with certainty, as the data could relate to several individuals, providing indistinguishability amongst them.

Query text does not need to be covered by metadata generalisation

(674) The query text does not need to be covered by the metadata generalisation to achieve *k*-anonymity. This is because, as is set out below, the query text should not be considered a quasi-identifier in the data sharing context of Article 6(11) of Regulation (EU) 2022/1925. Additionally, query text does not lend itself well to linking attacks, as the large amount of variety in possible query text formulations make such linking highly uncertain. For example, even if an attacker knew that an end user is looking for white sneakers, the query text could still take many forms, which the attacker has no way to predict (e.g.: "*white sneakers*", "*sneakers white*", "*buy white sneakers*", "*withe snaekers*" – to name a few). This makes using the query text for linking attacks complex and difficult to do at scale.

(675) Alphabet's anonymisation approach (see section 4.4.2) applies metadata generalisation that covers both the metadata and the query text. This means that at least five users with identical metadata must have issued the exact same query. Including the query text in the metadata generalisation results in a large amount of data suppression, greatly degrading the quality and usefulness of the data in a way incompatible with the objective pursued by Article 6(11) of Regulation (EU) 2022/1925. This is because query text can take many possible values (there are many variations in which even similar queries can be formulated), meaning there are many unique queries. Therefore, requiring even five query texts to be identical *and* have identical metadata excludes many queries: this step taken in isolation removes more than [90-100]% of query-metadata combinations.

(676) Alphabet argues that not generalising the combination of a given query and its metadata leaves search records exposed to re-identification. Alphabet argues that at

---

1014 For instance, Alphabet reports that more than [number of unique signed-in users] unique signed in users issued queries in French from a mobile device in a single day in NUTS3 region FR101, which corresponds to central Paris. See Alphabet's response to RFI 12 dated 11 May 2026, Doc ID […], question 6.

1015 Alphabet's response to RFI 12 dated 11 May 2026, Doc ID […], question 6.2. This assumes that every unique signed-in user appears in a single metadata bucket, and the metadata generalisation measures, which may combine or suppress buckets that do not meet the threshold, have not been applied.

least [80-90]% of queries are unique (issued by a single user)[1016], meaning that users may be singled out.

(677) As set out in recital (574), Alphabet's assessment of the re-identification risk stemming directly from the query text largely follows from its incorrect interpretation of the legal standard. Alphabet considers that the technical measures by themselves should reduce the re-identification risk to insignificant level, and that all personal data should be anonymised, rather than only end users' personal data. Under this premise, Alphabet considers the query text a quasi-identifier that must be subject to metadata generalisation. As a result, Alphabet's interpretation is not in line with the legal framework set out in section 4.4.1. Under the correct legal interpretation, the query text need not be considered a quasi-identifier.

(678) A quasi-identifier is a piece of information that could be used, either individually or in combination with other quasi-identifiers, by someone that has knowledge about that individual with the purpose of re-identifying the individual in the dataset.[1017] Unlike quasi-identifiers such as postal code or birth date, the exact query text issued by a given individual is unlikely to be an attribute about that individual that an attacker already knows, and can use in an attack. As Alphabet points out, the query text is an open-ended data field that can take any value.[1018] In practice, most search queries are not directly related to personal characteristics about the user, and instead concern general topics (weather, sports, news, culture, etc.). Even attackers with knowledge about an individual are very unlikely to know of the exact query text issued by that individual: if the attacker would know about topics that an individual is likely to have queried, the syntactic diversity of query text means that the exact query text can take a large number of values.

(679) Additionally, even if an attacker succeeds in using the query text as a quasi-identifier, this means they already know what a user was searching for. As a result, in this scenario, it is unlikely to lead to meaningful information gain. As set out in section 4.4.4.1.2.1.2, the Search Data is not organised in sessionised form, but as loose queries. This means that if the query text is known, there is likely little additional information to be gained.

(680) In summary, the query text should therefore not be considered a quasi-identifier subject to metadata generalisation in this context. As explained in section 4.4.4.1.2.1.7, Alphabet has not demonstrated that the query text – following the query suppression measures – poses a risk of re-identifying end users beyond a residual level. Alphabet has not shown a single targeted attack using the query text (or any targeted attack at all), nor has it demonstrated that it can pick a random query and re-identify the end user with significant likelihood and certainty. Furthermore, the query text is an open-ended field which can take any value – making it less suitable for attacks at scale.

(681) Alphabet further argues that upleveling metadata fields does not provide suitable protection against re-identification. This is surprising, as Alphabet applies such upleveling in its own anonymisation approach (see recital (563)(c)). Alphabet illustrates its point with the hypothetical example of a Finnish language query about an abortion clinic issued in Portugal ("*abortion clinic near Afurada*"). Alphabet argues that the combination of query text, location, day and language leaves the user

---

1016 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 111.

1017 See https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf. (last accessed on 28 May 2026), Doc ID […].

1018 Alphabet's response to the Preliminary Findings, Doc ID [...], Section II.B.

vulnerable to re-identification but does not explain how it would achieve such re-identification.

(682) Compared to the Preliminary Measures, the specified technical anonymisation measures in the present Decision apply less upleveling, which strengthens protection. The measures now only uplevel the location of a query from a NUTS3 region to country. In addition, inferred language and device type are now made non-generalisable, which means that queries in a given language and for a given device type that do not meet the metadata threshold on a country-level are suppressed. This mitigates the risk of device type being inferred from interaction data, which may otherwise undo generalisation of this attribute.

(683) The stricter approach presented in the previous recital means that, considering Alphabet's example, at least 1,000 unique users must have issued queries in Finnish on a given day for the queries to be released. Otherwise, the queries are not provided at all. It is entirely unclear from Alphabet's example how an attacker would succeed at identifying the Finnish user searching for an abortion clinic among at least 1,000 Finnish users active in Portugal that day. Even if the query text may suggest a more precise location – as is the case in Alphabet's hypothetical example – an attacker has no way of knowing how many of the other Finnish users are in the same location.

(684) In addition, Alphabet's position that a granular inferred location in the query text (or result URL) "undoes" the metadata generalisation is reductive. The objective of metadata generalisation is not only to coarsen the location of each query. Metadata generalisation ensures that users are clustered into groups of at least 1,000 – which prevents re-sessionising queries of users with rare characteristics, such as those using a rare language or living in a sparsely populated area. For example, Finnish queries in Portugal will only be released if at least 1,000 unique signed-in users issued queries in Finnish in Portugal on a given day. A single query with a more granular location, such as a Finnish query text referring to a town in Portugal, does not undo that – the query could still stem from any unique user within the group.

Result URLs do not need to be covered by metadata generalisation

(685) The Expert Report on Anonymisation proposes an additional metadata generalisation step, which generalises metadata relating to URLs that received fewer than five clicks to further reduce the risk of linking attacks using auxiliary datasets.[1019] As pointed out in the report, while this step is conservative, as it mitigates a privacy risk that is comparatively minor, it has a large impact on the data quality and usefulness: more than [90-100]% of daily unique URL clicks and [60-70]% of daily unique domains would be removed entirely.[1020] The Commission considers that this step would substantially degrade the quality and usefulness of click data, thereby seriously undermining the objective pursued by Article 6(11) of Regulation (EU) 2022/1925, while not being required to reduce the overall risk of re-identification to an insignificant level in light of other technical measures and complementing contractual measures to ensure anonymisation. More specifically, in reaching that conclusion, the Commission assessed together the practical feasibility of linking attacks in light of the technical measures applied to the Search Data, the information gain that could reasonably be obtained from a successful linking attack and the extent to which the contractual measures further reduce the likelihood that third-party OSE recipients would seek to carry out such attacks in this specific context.

1019 Expert Report on Anonymisation, Doc ID […], paragraphs 305-308.

1020 Expert Report on Anonymisation, Doc ID […], paragraphs 371, 376.

(686) First, as set out in recital (622)(b), the linking attacks targeted by the URL generalisation measure are only possible where precise and already revealing auxiliary information is available, which strongly limits the scope of these linking attacks in the context of Article 6(11) of Regulation (EU) 2022/1925. The scope of such attacks is already reduced by the proposed technical measures, which either remove URLs entirely (e.g., query suppression), or aggregate associated metadata, making it harder to identify which records to link to the available auxiliary dataset for both third-party OSE beneficiaries and other unintended recipients. As described above, the metadata generalisation has been significantly strengthened, thereby further reducing the risk of linking attacks. It follows that any remaining attacks based on result URLs would require particularly specific auxiliary information and would concern only a limited subset of records.

(687) Second, as direct identifiers have been removed from the Search Data, the information gain from a linking attack with an auxiliary dataset (or other types of linking attacks) appears minimal, as only an individual query can be linked to the information already available in the auxiliary dataset. For example, if a third party holding auxiliary data for a web shop selling shoes were to accurately and successfully link a record in the Search Data, it may find a query text such as "*black sneakers*" – this is likely to provide very limited additional information to the information already contained in the auxiliary dataset. As set out in recitals (754) – (758), re-sessionising queries, in particular across topics, is very unlikely to be feasible. It follows that the information gain that could reasonably be obtained from a linking attack based on URLs is, in most cases, so limited that it could only marginally contribute to increasing the risk of re-identification of end users.

(688) Third, while third-party OSE beneficiaries might, in theory, have the commercial incentive to attempt to link query text to auxiliary data (e.g., to understand the terms search by users that visited a specific website), this would directly contradict the contractual *effective control, segregated processing environment and prohibitions against re-identification, linking and augmentation*, and *permitted purposes of use* measures provided for in recitals (819) to (822) with the result of being exposed to the suspension of access to the Search Dataset (see section 4.6.7.2). Those measures ensure that the Search Dataset remains technically segregated from any other auxiliary datasets available to the third-party OSE, being its own search dataset, advertising dataset or other. For all the reasons explained in recitals (885) to (891), the Commission considers that the incentive structure created by Article 6(11) of Regulation (EU) 2022/1925, together with the implementing act under Article 8(2) specifying the legally binding conditions under which Alphabet must grant access to the Search Dataset, ensures that, in this specific context, the commercial incentives of third-party OSEs are aligned with maintaining continued access to the Search Dataset rather than engaging in such linking attacks, a conduct that would jeopardise such access.

(689) In its response to the public consultation, the EDPB encouraged the Commission to assess if additional technical measures could be envisaged to "*further mitigate the residual risk of re-identification*" in relation to click data. The EDPB mentioned possible measures aimed at further transforming the sequence of viewed URLs/blocks, including by shortening/truncating URLs or introducing a threshold for removal, or adding noise to click data. The Commission has considered such possible measures. It finds that measures which shorten the URLs inevitably degrade data quality and usefulness extensively, because even at domain level, [60-70]% of daily URL clicks are unique (see recital (685)) – meaning most URLs would need to

be suppressed fully to implement such measures. Furthermore, while the measures specified in the present Decision coarsen click-back timing and duration of interactions such as scrolls and hovers (all defined as click data under section 4.3.2.3), adding noise to URL clicks (e.g., reporting additional fictional clicks) is bound to create inaccurate signal in the dataset that would harm the optimisation of search services.

(690) However, the measures specified in the present Decision introduce alternative measures that contribute to mitigating risk from linking attacks. As mentioned above in recital (664), the revised measures include larger metadata buckets and coarser location information, which further reduce the residual risk attached to click data as it becomes far less likely that an attacker can obtain meaningful additional information from the query on which it already has auxiliary data. In addition, the specified contractual *effective control, segregated processing environment and prohibitions against re-identification, linking and augmentation* measures are specifically aimed at addressing risk of linking based on auxiliary data (see recitals (819), (820) and (821)).[1021] Together, these measures effectively mitigate risk stemming from linking attacks.

(691) Alphabet argues that the metadata generalisation must be applied to result URLs. Alphabet explains that in addition to linking attacks on clicked URLs – which is addressed above – result URLs can convey information about a user's location, they can reveal personal information saved in a user's Google account (e.g., a Maps link with directions to a home address), and personalised results can reveal information about a user's interests. However, these arguments do not invalidate the metadata generalisation applied in the measures:

(a) Concerning result URLs that convey information about a user's location, Alphabet presents the example query "*restaurants near me*". Alphabet argues the results for this query are likely to indicate an end user's location with high precision – even if the location metadata field is generalised. This argument again misrepresents the objectives of metadata generalisation (see recital (684)). Metadata generalisation does not just serve to obfuscate end user location – it clusters users in groups of at least 1,000 with the same metadata to prevent re-sessionisation. Therefore, even if a specific query text includes a more granular location, the larger groups resulting from the revised metadata generalisation still limit the risk that these queries are re-sessionised with other queries, leading to information gain.[1022] For this to be successful, the more granular location needs to be inferable for multiple queries with enough precision to determine that they belong to the same end user.

(b) Concerning result URLs that incorporate information saved in an end user's Google account (e.g., Google Maps links providing directions to home), the specified measures in the present Decision require Alphabet to suppress such URLs (see recital (637)(f)), fully addressing risks stemming from these URLs.

(c) Concerning personalised results, Alphabet argues those can reveal additional information about a user once identified – but this skips over a key step: actual

---

1021 Contrary to Alphabet's argument in Annex 3 to its response to the Preliminary Findings, Doc ID […], (paragraphs 105-110), daily releases of data do not have a material impact on the likelihood of successful linking attacks. As the report sets out in paragraph 108 [Alphabet's internal data].

1022 Furthermore, the revised measures suppress results that directly include locations stemming from an end user's Google account and results incorporating a user's exact location (e.g., navigation directions), thereby excluding result types that provide verifiable and exact end user locations.

re-identification of the user. Alphabet has not demonstrated any plausible re-identification attacks that employ the personalised ranking of a result. Alphabet only presents a hypothetical example where an end user issues the same query in Google Search and a recipient search engine. Alphabet argues that the recipient could then link the queries and learn additional information about the user from personalised results. However, this hypothetical attack fully ignores the contractual measures, which require recipients to segregate the Search Dataset and forbid linking with own search data (see section 4.4.4.2.2). Moreover, attackers do not even have a way to detect whether a result is personalised or not – greatly reducing their utility as an attack vector.

(692) Alphabet further argues that ads URLs can convey information about a user, rendering them re-identifiable (see also recital (637)(d)). The specified measures in the present Decision require Alphabet to suppress all ad URLs, fully mitigating any risk stemming from such result URLs.

User interaction does not need to be covered by metadata generalisation

(693) The metadata generalisation does not need to cover interaction data such as clicks, dwell time and hover time to achieve *k*-anonymity. This is because such interaction data is not a quasi-identifier. However, the revised technical measures coarsen interaction data by replacing the exact timing with ranges (see recital (670)). This conservative approach prevents that exact interaction timing is used to create behavioural fingerprints of users, which may be used for a re-sessionisation and subsequent re-identification attack.

(694) Alphabet argues that the metadata generalisation should cover user behaviour data to prevent attackers from observing such behavioural patterns in the data. The coarsening measures in the present Decision, which replace exact interaction durations with bins based on percentiles of the distribution of these durations in a given metadata group (see recital (670)), prevent behavioural fingerprinting, as these bins ensure that the Search Data provide the same range of interaction durations for a significant number of end users.

4.4.4.1.2.1.5. Mini-sessionisation

(695) The technical anonymisation measures require Alphabet to link together queries into very limited sessions ("mini-sessions"), provided the follow-up queries are refinements of the earlier query. This step provides beneficiaries with valuable data for query analysis (e.g., refinements show the true intent behind the initial end user query), while preventing the privacy risks associated with releasing full session data.

(696) OSEs habitually group search records into sessions from the same end user. This provides context to queries which is valuable to optimise OSEs. For instance, when the end user issues a series of queries in quick succession, it often indicates the end user did not find what they were looking for, prompting them to refine their query text. This end user behaviour provides valuable insights to online search engine providers, enabling them to better understand the end users' intent behind ambiguous queries and provide end users with relevant information and proactive suggestions to further refine their search.[1023]

(697) While using fully sessionised data to optimise OSEs in the same way that Google search does would be useful for beneficiaries, the Commission's anonymisation approach does not allow for the releasing of full sessions in the Search Data given

[1023] Expert Report on Anonymisation, Doc ID […], paragraphs 242-243.

the high privacy risk that this would entail. Indeed, the Commission's first attribute suppression step removes Google account identifiers (e.g. account IDs, usernames) and other associated direct identifiers (e.g. IP addresses, device IDs) from all search records (see recital (596)).

(698) However, many sessions consist of end users refining their query, e.g., searching for "*carrot cake*" and immediately afterwards searching for "*carrot cake vegan*". Such refinements could be additions typed by the user or could be through a query modifier suggested by Google Search. Combining both query search records does not result in significantly more privacy risk than considering only the second record. For example, in the case of additions, the preceding queries do not contain information that is not already present in the subsequent refined query. As each subsequent query is strictly an addition or a Google Search provided suggestion based on the previous query text, the only information that the preceding queries convey is how a user refined the query to come to the final query. For instance, if an initial query "*carrot cake*" is followed by "*carrot cake vegan*", the initial query does not provide information that is not in the refined query.

(699) In line with the above, the Commission's preliminary technical measures allow such limited session-level data to be shared in "mini-sessions". Mini-sessions are sessions where the queries following the initial query are strictly refinements of the previous query (e.g. a user addition, clicking on a query refiner, or selecting an autocomplete option). The length of mini-sessions is capped at three queries.

(700) Mini-sessions provide useful session data to beneficiaries while avoiding aggregating end user queries on multiple unrelated topics, which would increase the amount of information an attacker could use to re-identify end users and to learn new, previously unknown information in the process.[1024]

(701) By requiring each subsequent query to be a refinement, preceding queries are related to each subsequent query of the mini-session. This means that mini-sessions are a privacy preserving way to share limited session data with recipients.

(702) Alphabet argues that mini-sessions expose users to re-identification as a Google Search suggestion can lead an end user to wander through various topics. Alphabet additionally argues that it has identified mini-sessions of up to 200 queries long.

(703) First, the revised measures in the present Decision cap the length of mini-sessions to three queries. This limits the variety of topics that a user could drift to.

(704) Second, Alphabet does not dispute that mini-sessions consisting of sub-strings of the final query do not convey additional information to what is provided in the final query – this represents [50-60]% of all mini-sessions.[1025] In the case of a strict substring-superstring relationship, there is virtually no risk of an end user drifting between topics within a mini-session. To take the earlier example, a mini-session may contain the query "*carrot cake*", followed by "*carrot cake vegan*". These are about the same topic.

(705) For the remaining [40-50]%, users have clicked refiners, which may take the user to a different, yet related topic. These topics are proposed by Google Search as related topics and not formulated by the end user (e.g., "*cheese*", "*mozzarella*", "*Italian Mediterranean buffalo*"). This makes it less likely to be identifying – the related topics proposed by Google Search are closely related to the previous query, and they

1024 Expert Report on Anonymisation, Doc ID […], paragraphs 246-248.

1025 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 223.

are based on what many other users have searched for. Capping the length at three queries further limits the potential for an end user to drift far from the initial topic.

(706) Alphabet additionally argues that limiting mini-sessions to three queries only truncates them, and that they can still be combined into longer sessions.[1026] This is incorrect, as clicked modifiers from the last query of a mini-session are suppressed, meaning that attackers would not be able to rely on those to link the mini-sessions together. Furthermore, queries can be part of at most one mini-session, meaning that there can be no overlapping mini-sessions that could be pieced together by an attacker.

(707) Last, Alphabet has not presented any examples of re-identification based on mini-sessions. Alphabet has only shown a hypothetical example of Google Search refinements leading a user through different topics.

4.4.4.1.2.1.6. Other measures

(708) The specified measures require Alphabet to communicate certain implementation details on the anonymisation measures to the Commission for review, within the time limits set out in section 4.6.4. This creates transparency on how the technical anonymisation measures are implemented and ensures that the implementation choices are appropriate. This reporting concerns three matters:

(a) **Personal data detectors:** the query suppression step requires the use of personal data detectors for entity recognition (see section 4.4.4.1.2.1.3). There are several parameters relating to these detectors that can affect the effectiveness and proportionality of this measure. For instance, which personal data detector technology is used, which specific detectors are used, and what likelihood thresholds are used when applying the detectors. Alphabet must report these choices to the Commission for its review and explain the rationale behind each of these choices.

(b) **Results relating to Google services or precise end user location:** the attribute suppression step requires Alphabet to suppress result URLs that directly incorporate end user information saved in the Google account (e.g. home address), and results that use the end user's precise location (e.g., directions). During the proceedings, Alphabet has only identified Google Maps URLs as a result type that incorporates such information, but indicated that it cannot exclude additional cases. This reporting step ensures that result URLs are only removed from the Search Dataset where appropriate.

(c) **Computing resource cost:** Alphabet must report to the Commission the computing resource cost to implement each of the anonymisation measures. This creates transparency on the relative costs per step and facilitates regulatory dialogue during the implementation of the technical anonymisation measures. Where different implementation options are possible which offer equivalent privacy protection, Alphabet must choose the least costly option so that the cost of the Search Dataset is not higher than strictly necessary.

(709) The measures require Alphabet to provide to eligible recipients, on a quarterly basis, key information in relation to the anonymisation of the Search Dataset. This publication creates transparency on how the Search Dataset is impacted by the anonymisation process to third-party OSEs before they decide whether to acquire the

[1026] Alphabet's response to the Revised Measures, dated 15 June 2026, Doc ID […], footnote 10.

data. The reporting requirement covers two areas in relation to the anonymisation process:

(a) The use of personal data detectors for query suppression (see section 4.4.4.1.2.1.3). Personal data detectors play an important role in how the query suppression step is implemented, and it is therefore important for both the Commission and potential data recipients to have transparency on how Alphabet has implemented this measure. Providing these details allows both the Commission and recipients to monitor and challenge the effectiveness of these detectors.[1027] The measures also require Alphabet to use publicly available personal data detectors. This makes Alphabet's methodology reproducible and allows third parties to experiment with the detectors that Alphabet uses.

(b) The proportion of unique queries and query volume suppressed and altered by the anonymisation process per measure. This shows how the different specified measures affect the Search Dataset, which may be a relevant factor in how third-party OSEs choose to use the data. The lack of visibility on how Alphabet's current anonymisation proposal affects the Google Search Data has been a pain point among third-party OSEs so far. As Alphabet was unwilling to share statistics on the amount of data altered and suppressed, [market participant] was required to run experiments with its own data to get an estimation, which only gave an uncertain estimation, as statistics can heavily and non-linearly depend on data volume (e.g., proportion of long tail queries).

(710) New data attributes that fall within the data scope of Article 6(11) of Regulation (EU) 2022/1925 may be introduced by Alphabet over time. Such new attributes will not have been considered in the design of the anonymisation measures in the present Decision and may raise re-identification risks. The measure provides that when Alphabet introduces new data attributes that are to be shared as part of the Search Dataset, it must assess whether they pose a re-identification risk. If so, Alphabet must propose appropriate anonymisation measures to the Commission in relation to that attribute. The proposal must be substantiated with a clear explanation of the re-identification risk and its magnitude (e.g., the number of records affected), and the impact of the proposed anonymisation measure (e.g., the number of records that will see the new attribute altered or suppressed. In line with recital 61 of Regulation (EU) 2022/1925, the anonymisation measure should not unnecessarily affect the quality and usefulness of the data.

4.4.4.1.2.1.7. Testing of the technical anonymisation measures

(711) Alphabet argues that insufficient testing of the Commission's technical anonymisation measures has been conducted.[1028] Alphabet also claims that it has performed red team testing of the Commission's preliminary measures, and that this surfaced serious vulnerabilities.

(712) Contrary to Alphabet's claims, the Commission has performed testing of its anonymisation measures. The Commission's testing consists of two phases: (i)

1027 The EDPB stressed the importance of this in its comments on the proposed measures of 5 May 2026, Doc ID […], paragraph 23.

1028 Alphabet argues that testing is particularly important here, as it characterises the proposed technical measures as "*ad hoc*". As set out in recital (626), this is not the case – the technical measures are based on well-established principles and techniques.

specific tests to inform the design of the technical anonymisation measures,[1029] and (ii) tests on a dataset covering one week of Irish search queries to assess whether its preliminary technical anonymisation measures are effective in reducing the re-identification risk to a residual level in line with the guiding principles set out in recital (619) and taking into account Alphabet's testing results (see recitals (748) to (758) below); This testing is in addition to the testing that Alphabet performed and the Commission's detailed review of Alphabet's results (see recitals (721) to (747) below).

(713) The data required to conduct thorough testing of any anonymisation approach is by nature under Alphabet's exclusive control. This makes Alphabet uniquely positioned to test any anonymisation approach. Requiring Alphabet to take a key role in the testing is therefore not, as Alphabet purports, an impermissible shift of the burden of proof[1030] – it is not more than logical, and even necessary, for Alphabet to take an active role in the testing of preliminary measures. Alphabet has performed testing of the preliminary measures (see recitals (748) to (758) below), which the Commission has carefully reviewed. In response to the testing performed by Alphabet, the Commission has made several changes to the preliminary anonymisation measures, these include changes to the metadata generalisation threshold, suppression of ad URLs, limiting mini-sessions, as well as others. Where the scenarios set out in Alphabet's testing did not raise concerns about the preliminary anonymisation approach, the Commission has explained why this is the case below.

(714) While Alphabet is in a position to test under optimal conditions, the testing that the Commission can conduct is dependent on Alphabet's willingness to provide the Commission with effective data and tools in a timely manner. In this respect, the Commission's testing was hindered and delayed by Alphabet's reluctance in providing the Commission with the requisite data.

(715) Alphabet claims that the Commission has had the requisite data in its possession since May 2025 and therefore has had close to a year for testing.[1031] However, as explained above in recital (67), the data provided was not provided in full until November 2025. Furthermore, the data requested in May 2025 did not comprise the information needed to test the Commission's anonymisation measures, which had not yet been devised (although the collection of input and preparatory work was ongoing). Instead, this data was requested to better understand the impact of Alphabet's anonymisation approach on the quality and usefulness of the Google Search Data. This is well known to Alphabet, as evidenced by its description of the testing environment: "*Google set up the RIDGE environment in May 2025, well before the Specification Proceedings were opened, as a means to provide access to search data in response to an RFI. It was never intended as a platform for privacy testing*".[1032]

(716) The relevant reference point is instead the Commission's request for information of 11 February 2026, which requested the data necessary to perform testing of the Commission's measures.

1029 For example, RFI 11 of 12 November 2025, RFI 1 of 6 February 2026, RFI 6 of 13 February 2026, among others, contained detailed questions on the characteristics of the Search Data, such as the distribution of query length, the effect of word- and length-based thresholds, and user interactions with result URLs.

1030 Alphabet's response to the Revised Measures, dated 15 June 2026, Doc ID […], section II.B.

1031 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 232.

1032 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 8.

(717) Alphabet replied to the Commission's request for information of 11 February 2026 in two instalments, on 13 March 2026 and 31 March 2026. Technical issues meant that the Commission's experts only effectively gained access to the full response on 8 April 2026. However, issues with the cloud environment in which the data was made available persisted, and there were numerous exchanges between the Commission and Alphabet to resolve these. The time it took Alphabet to provide effective access to the data and occurrence of frequent technical issues[1033] stand in stark contrast with the speed at which Alphabet was able to implement the Preliminary Finding's anonymisation measures for its own testing. Within two weeks of the adoption of the Preliminary Findings, Alphabet approached the media with claims that it had been able to reverse-engineer the preliminary anonymisation approach. This suggests that these two weeks were sufficient for Alphabet to apply the anonymisation measures to a data sample *and* perform testing on the data, while it took close to two months to implement partial elements of the technical anonymisation measures and make sample data available to the Commission.

(718) Alphabet argues that the Commission's issues with the cloud environment are unfounded and that its own external experts did not experience such issues when using the environment.[1034] While the Commission cannot verify whether Alphabet's external *experts* experienced issues, the fact is that most of Alphabet's testing was performed by 10-15 *internal* engineers, which did not need to rely on this environment. The testing report produced by the Commission's experts documents the issues and limitations that they experienced.[1035] Nonetheless, the report concludes that the testing produced conclusive results which support that the technical measures play a prominent role in mitigating end users' re-identification risk associated with the presence of their personal data in queries, and of re-sessionisation attacks and reduce this risk to a residual level in line with the guiding principles set out in recital (619) above.

1033 To achieve effective access to the dataset, first, the Commission's contractors needed to be granted access to Alphabet's cloud environment that hosts the dataset. In preparation for the analysis, the Commission asked Alphabet to provide accounts for the environment on 4 March 2026 (Doc ID […]). It was only on 17 March 2026 that Alphabet informed the Commission that the environment had reached the maximum number of accounts and asked which ones the Commission no longer needed (Doc ID […]). There is no good reason why Alphabet did not ask this simple question from the start. On 20 March 2026, one of the Commission's contractors managed to gain access to the environment, but still faced technical issues since Alphabet had not yet granted the right permissions to access the hosted dataset (Doc ID […]). After a reminder of the Commission on 23 March 2026 (Doc ID […]), the contractors gained access to (i.e. the ability to view and query) the tranche 1 dataset in the environment on 24 March 2026 (Doc ID […]). Alphabet continued to be late in providing information to the Commission. For example, the Commission requested in a call with Alphabet on 7 May 2026 access to the dataset that Alphabet had used for the testing of the Commission's preliminary measures, after which the Commission followed up in writing on 11 May 2026 (Doc ID […]). After sending two reminders on 19 May 2026 (Doc ID […]) and 26 May 2026 (Doc ID […]), it was only on 27 May 2026 (Doc ID […]) that Alphabet asked the Commission's request to be put in an RFI, a request Alphabet could have made soon after the Commission's initial question. The Commission sent the RFI on 28 May 2026 (Doc ID […]). Another example of suboptimal set up of the platform and undue delay occurred when, on 22 April 2026, the Commission requested to Alphabet the ability to store intermediary outputs to improve analysis of the accessed data (Doc ID […]). Alphabet only made available the possibility to store intermediary outputs on 3 June 2026 (Doc ID […]).

1034 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 8. In the same paragraph, Alphabet argues that the platform was never intended for privacy testing, which is at odds with Alphabet's own external privacy experts using it in that way.

1035 DMA 6(11) anonymisation strategy: testing and parameter evaluation (the "Anonymisation Testing Report"), Doc ID […], pages 3-5.

(719) Monitoring and testing of the effectiveness of the anonymisation measures is not limited to the present proceedings. As the anonymisation measures in this case are rolled out, the Commission will be able to consider real-world experience with the dataset as well as the results of further testing:

(a) The Decision anticipates a biennial review of the measures, which takes on board real-world experience with the Search Dataset, additional testing (be it by Alphabet, third-party OSE recipients or the Commission) and technological advances that may affect the likelihood of re-identification of the Search Dataset.

(b) At any time, Article 8(9) of Regulation (EU) 2022/1925 allows the Commission to reopen proceedings where there has been a material change in any of the facts on which the decision was based, including in the form of results from new monitoring and testing of the effectiveness of the anonymisation measures such as independent third party evaluation taking also into account the feedback from the civil society. Such material change may justify amendment or change of the anonymisation measures. The Commission will assess any such new facts within the framework and principles set out in this decision.

(c) Regulation (EU) 2022/1925 also provides scope to react to urgent vulnerabilities that come to light after adoption of an implementing act under Article 8(2) of that Regulation. For instance, Article 10(4) of Regulation (EU) 2022/1925 allows the Commission to suspend the application of a specific obligation, fully or partially, in the case of urgency.

(720) In the below, the Commission sets out its review of Alphabet's testing of the anonymisation measures ("**Alphabet's testing**"), as well as a summary of the Commission's own testing and the Commission's analysis of Alphabet's response to that testing.

Assessment of Alphabet's testing

(721) Alphabet performed testing on one week of Irish search data on which it applied the technical anonymisation measures proposed in the Preliminary Findings. This exercise took place between Alphabet receiving the Preliminary Findings on 16 April 2026 and Alphabet's reply to the Preliminary Findings, which it submitted on 18 May 2026 and included an annex with the testing results. Alphabet submitted further testing in its reply to request for information 15 on 29 May 2026 and as part of its observations on the Commission's testing report on 17 June 2026, indicating that testing continued after the submission of the reply to the Preliminary Findings – a period of at least 2 months. Alphabet indicated that it has dedicated significant computing resources requiring management approval, a team of 10-15 engineers as well as external experts in the testing. Alphabet claims that during the exercise, it was able to re-identify several individuals in under two hours.[1036] However, as this section sets out, all risks identified by Alphabet can either be considered below residual level based on the guiding principles set out in recital (619) above or have been addressed in the specified measures in the present Decision.

[1036] Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […]. The Commission requested the relevant data and source code to review Alphabet's testing in a meeting on 7 May 2026. Alphabet only provided access to the data on 29 May 2026, meaning the Commission primarily relied on Alphabet's testing report submitted as annex 2 to Alphabet's reply to the Preliminary Findings to evaluate the red team testing.

(722) Alphabet's testing does not reflect an end-to-end simulation of a realistic attack. As potential third-party OSE recipients have put it: "*The Red Team report only considers the technical measures, completely disregarding the contractual measures that will be layered on top.*"[1037] Alphabet performed atomic adversarial attacks in an environment without the security controls, logging, or incident detection prescribed in the contractual measures, which would be present in a real-life attack. Alphabet specifically examined the path that a large group of highly skilled experts with existing knowledge about the dataset would take if given unlimited compute power, no logging, no incident response, and none of the additional safeguards set out in the contractual measures. This does not correspond to a realistic attack scenario. According to Alphabet's own documentation, such a set-up should be characterised as "adversarial testing" and not as red team testing.[1038] Alphabet's testing therefore did not follow the best practices and standards of most red team definitions, such as mimicking real-world attacks with a realistic scenario.[1039] It follows that Alphabet's testing provides useful input on potential worst-case scenarios. However, it constitutes a partial assessment, not taking into account all the circumstances of the specific data sharing under Article 6(11) of Regulation (EU) 2022/1925.

(723) As set out in section 4.4.4.1.2.1.1, a risk is considered beyond residual if it is possible to (i) choose a specific individual and, with significant probability, retrieve some of their search records with high certainty; (ii) choose a random search record and, with significant probability, re-identify the end user with high certainty; or (iii) perform attacks that re-identify a large number of end users with high certainty and with reasonably simple methods. Alphabet's examples do none of these three:

(a) Re-identifying a specific individual is also known as a targeted attack. Alphabet's testing has not presented a single example of a targeted attack.

(b) Being able to re-identify random search records with high probability is an example of an untargeted attack. Alphabet's testing has not demonstrated that this is possible. Instead, all examples of re-identification by Alphabet are carefully selected worst-case queries – often edge cases – not random queries.

(c) Re-identifying a large number of end users with high certainty and reasonably simple methods is another example of an untargeted attack. While Alphabet's testing has shown examples of re-identification, these have not been at scale. Furthermore, as will be set out below, Alphabet's examples primarily target carefully selected worst-case queries and therefore are unlikely to be scalable.

1037 [Market participants]written submission of 9 June 2026, Doc ID […], page 3.

1038 See for example the Google blog titled "*Why Red Teams Play a Central Role in Helping Organizations Secure AI Systems",* Fabian, D., & Crisp, J. (2023). Available at https://services.google.com/fh/files/blogs/google_ai_red_team_digital_final.pdf (last accessed on 17 June 2026), Doc ID […]. In this blog Alphabet says: "*At Google, we generally use "red teaming" to mean end-to-end adversarial simulation, that is taking on the role of an attacker who is trying to achieve a specific goal in a specific scenario. In contrast, adversarial testing can be much more atomic, and more appropriately applied to the individual parts that make up a complex system.*" Alphabet also emphasises: "*The main point is for the red team to emulate the same behaviors a real threat actor would use in a real-world scenario to gain a foothold and remain undetected.*" In this case, the real-world scenario would include the protections, logging, and detections required to be put in place.

1039 See for example https://www.ibm.com/think/topics/red-teaming (Doc ID […]) and https://csrc.nist.gov/glossary/term/red_team (Doc ID […]), last accessed on 17 June 2026.

(724) The first vector of attack identified by Alphabet is re-identification directly based on the query text. Alphabet presents examples of full names in query text and residential addresses in query text.[1040]

(725) The fact that full names remain in the query text is not surprising. As set out in section 4.4.4.1.2.1.3, the entity-based thresholds do not attempt to exclude all names from the query text. Names are in most cases from individuals other than the end user issuing the query, meaning it is not in scope of the anonymisation requirement set out in Article 6(11) of Regulation (EU) 2022/1925. Even in cases where a search is a self-search, it is often hard to detect this. It is telling that all Alphabet's examples are queries in the form "*my name is …*": this illustrates the difficulty of correctly identifying self-searches. Overall, search queries with this format can likely be considered an edge case. Furthermore, this format of query may still not be conclusive evidence that the search is a self-search,[1041] and unless additional information is provided in the query text, it does not provide any additional information besides a full name.

(726) Alphabet indicates that its examples of addresses in the query text concern home addresses that passed the query suppression. While such examples certainly exist, the address must in addition relate to a single-family home for which the occupant can be confirmed.[1042] Indeed, while names and addresses in the query text are undoubtedly personal data relating to the individual who lives at that home address, the query text cannot be attributed with high certainty to the individual who issued that query. The Commission's testing, summarised in recitals (748) – (758), confirm that names and addresses in the query text are unlikely to pose significant risk of end user re-identification.

(727) The second vector of attack presented by Alphabet combines the query text with the location metadata to re-identify end users.[1043] All Alphabet's examples in this category relate to pregnant persons, which Alphabet claims to be able to re-identify due to information provided in the query text on their employment. The technical measures specified in the present Decision set a metadata generalisation with a bucket size of 1,000, instead of the 50 proposed in the Preliminary Findings. Per Alphabet's own admission, this is effective to address such attacks: "*[m]any of our red-team attacks have been facilitated by starting from relatively small metadata groups and then slicing further with additional evidence. A larger metadata pool reduces the risk of these attacks.*"[1044]

(728) This bucket size is furthermore a strict lower bound, and most queries will be in buckets with significantly more signed-in users. Furthermore, the geographical subdivisions have been adjusted from areas that contain at least 1,000 users to areas with a population that is typically between 150,000 and 800,000. These adjustments together are a conservative step that create larger anonymity groups and further mitigate risks of the types identified by Alphabet in its testing, as it is far less likely that metadata such as location in combination with the query text identifies someone uniquely in such a large group.

1040 Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], Section II.

1041 The Commission's data exploration surfaced examples such as "My name is Earl", which is a tv show.

1042 Alphabet often used public land ownership records a s a proxy for finding the name of a person who lives at a certain address. However, this approach carries uncertainty and may be error-prone: the search may for instance concern someone renting the property or a temporary visitor.

1043 Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], Section III.

1044 Alphabet's Alternative Anonymisation Proposal, Doc ID […], page 4.

(729) The third vector of attack presented by Alphabet concerns re-sessionisation of queries based on a topic.[1045] Alphabet argues that it was able to link a group of queries belonging to one metadata bucket based on the topic of the queries and determine that these were likely to originate from the same end user. Alphabet has not demonstrated that it was ultimately able to re-identify the end user for any of the re-sessionisation examples. Furthermore, Alphabet's description of its experiment is unclear, as it does not show how it selected the relevant metadata bucket, how it performed the re-sessionisation, how many examples of suspected re-sessionisation it identified, and how many of those were incorrect – something Alphabet was only able to validate because it holds the full dataset.[1046]

(730) An additional experiment presented by Alphabet consists in using an LLM to link two distinct queries in the same metadata group that belong to the same end user. This experiment reports a high accuracy but is essentially meaningless: users often search for the exact same query multiple times and guessing that two identical or near-identical queries belong to the same end user will often be correct, despite providing no additional information to an adversary. Therefore, this experiment does not demonstrate meaningful re-identification risk: having two queries that say the same, or nearly the same, from the same end user offers no or very little additional information on an end user that could lead to re-identification.

(731) The Commission conducted two distinct experiments to evaluate re-sessionisation risk under more realistic settings (see recitals (754) – (758)). One measures the success of query linking attacks (i.e., successfully attributing queries to the same user so that more information is known about this user potentially increasing the risk that that user could be re-identified based on this information), controlling for query relatedness.[1047] It shows that re-sessionising unrelated queries (which could lead to high information gain, and therefore increased privacy and re-identification risk) is so difficult that the clusters formed by LLM approached the success rate of random guesses, and that linking even closely-related queries becomes very error-prone and uncertain with sufficiently large metadata buckets. The threshold of 1,000 specified in the present Decision is sufficient to make it highly unlikely that queries can be both re-sessionised and re-identifiable. Furthermore, the 1,000-threshold is a lower bound. Most end users will be in metadata buckets containing far more end users (see recital (664)).

(732) The second experiment shows that when attempting to find the worst-case query clusters (those who are at a higher risk of being potentially identifiable, and include sensitive information), these reconstructed sessions do not directly allow simple re-identification.[1048] Taken together, the experiments show that re-sessionisation is difficult to reliably perform at scale, especially in a way that enables meaningful information gain and that leads to successful re-identification.

(733) A fourth vector of attack presented by Alphabet concerns re-sessionisation of queries based on interaction time, in addition to topics.[1049] In one example, Alphabet was

---

1045 Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], Section IV.

1046 Furthermore, the slide in which Alphabet presented this attack, slide 11 of presentation "Initial reactions to the PFs' anonymization measures" dated 6 May 2026, gives a misleading representation of this attack. The attack is performed over metadata buckets covering 4 days. However, the slide only shows a small subset of the total number of queries (200 at the very least), to suggest the queries on the topic in question could be linked with ease.

1047 Anonymisation Testing Report, Doc ID […], Section 7.

1048 Anonymisation Testing Report, Doc ID […], Section 6.

1049 See Alphabet's response to RFI 15 dated 29 May 2026, Doc ID […], paragraphs 38-42.

able to combine topics and particularly short attention times to infer that some queries came from the same user, on metadata buckets with 50 to 100 users. Again, Alphabet does not demonstrate that these examples lead to increased re-identification risk. Additionally, it is unclear how Alphabet has selected the cases where it was able to perform the presented attack, and if an external attacker would be able to identify such worst-case examples without Alphabet's extent of data access. In any event, Alphabet's experiment was performed on metadata groups with 50 to 100 users, while the technical measures specified in the present Decision propose a minimum bucket size of 1,000, with coarse binning of interaction signals, which is a conservative step to further mitigate potential risk from this attack vector.

(734) Alphabet argues that this attack vector can be scaled up using LLMs, with attacks based on a combination of interaction timing and rare keywords.[1050] Alphabet does not provide any indication that such re-sessionisation attempts lead to increased re-identification risk and does not provide any information about how many queries were re-sessionised, nor how similar these queries are.[1051] Like the example outlined in recital (730), this does not demonstrate meaningful increased risk.

(735) Furthermore, the above analysis focuses on the smallest metadata buckets, which will contain at least 1,000 distinct signed-in users according to the specified anonymisation measures in the present Decision. But the coarser geographic areas, with a population that is typically between 150,000 and 800,000, will lead to significantly larger metadata buckets for most users in the dataset (see recital (664)). Furthermore, the inclusion of queries from signed-out users also increases the effective size of anonymity groups. This will render examples such as the one identified by Alphabet far harder to find, and potential re-sessionisation far more uncertain – making an attack of this kind far less realistic. In particular, in geographic areas with a population that is typically between 150,000 and 800,000 it is far less likely that only one end user issued queries for a given topic, and as the Commission's testing demonstrates, even re-sessionising queries within a topic is difficult (see recital (754) et seq.).

(736) A fifth vector of attack consists in a user repeating the exact same address query across metadata buckets, presumably to resume travel navigation. The address is provided without any additional context, so there is no clear indication that this is the end user's home address (as opposed to e.g. a friend or family member). An attacker would need significantly more information for a successful re-identification based on such a pattern of queries, and this would require manual and error-prone work that is difficult to scale. The associated risk can therefore be considered below residual level.

(737) The sixth vector of attack uses targeted ads to re-sessionise queries issued by the same end user. Alphabet identified the queries by looking for targeted ads with a top-level domain that suggests a different country than Ireland, and a language different from the query language. Using the full dataset, Alphabet was able to confirm that the queries indeed originated from the same user. The specified technical measures in the present Decision fully remove ad URLs (see section 4.4.4.1.2.1.2), thereby fully addressing this attack vector.[1052]

1050 See Alphabet's response to RFI 15 dated 29 May 2026, Doc ID […], paragraphs 43-45.

1051 Moreover, the experiment does not control for query relatedness, so the numbers might essentially be extremely close queries that do not reveal more information than if taken individually.

1052 This adjustment was also proposed by Alphabet in its alternative anonymisation proposal of 19 May 2026, Doc ID […].

(738) The seventh vector of attack uses result URLs that incorporate information that end users can choose to save to their Google account. In response to a navigation query such as "*home to place x*", Google Search may present a Google Maps URL that is prepopulated with the end users' home address. The specified technical measures in the present Decision require that Alphabet suppresses result URLs of this type (see section 4.4.4.1.2.1.2), subject to submitting a list of the concerned result types to the Commission for approval. This fully addresses this attack vector.

(739) Finally, Alphabet argues that attackers may perform an active attack that manipulates the integrity of the allow list. Alphabet argues that by issuing queries from sufficiently many accounts, attackers could "*perform large-scale surveillance operations and target the individuals as victims of crimes like identity theft and blackmailing*".[1053] Whether such attack is indeed "effortless" as Alphabet contends is debatable – an attacker would need to create fifty inauthentic accounts that avoid Alphabet's filters for invalid traffic. Furthermore, it is not clear how such an attack would subsequently allow profiling of an individual – only a small fraction of searches for full name are self-searches, and even then, may not contain additional information.

(740) Alphabet argues that a similar active attack is possible to ensure that granular location data is provided [location proxy]by issuing 1,000 queries from different accounts in that area. The effort needed for such an attack would be very significant – an attacker would need to issue queries from these 1,000 inauthentic accounts *every day*. In any event, the larger metadata buckets and the coarser geographic areas (with a typical population size between 150,000 and 800,000) included in the measures in the present Decision make such attack a lot more difficult to perform.

(741) Alphabet presented two additional testing results together with its observations on the Commission's testing results (discussed below in recital (759) et seq.).

(742) The first result concerns location data inferred from query text or result URLs. Alphabet claims that it is trivial to extract fine-grained location from these attributes, despite location data being provided in coarse NUTS3 regions. However, Alphabet does not quantify the proportion of queries affected by this or demonstrate a method for an attacker which does not have ground truth data to reliably infer location.

(743) It is not contested that some query text or results allow inference of a location that is more precise than the NUTS3 region. Alphabet incorrectly presents the presence of loose queries in a metadata bucket for which more precise location is inferable as proof that the generalisation of location data does not work. However, this is incorrect. The presence of such examples certainly does not undo the effect of the metadata generalisation. While inferring location data from query text may allow an attacker to gain a more granular location on that query, it does not enable the attacker to isolate all queries coming from that location within the metadata bucket. Re-sessionising queries based on more granular inferred location information would both require this information to be available across several queries in the metadata bucket and with enough precision to allow linking of these queries. As set out in recital (684), metadata generalisation ensures that users are clustered into groups of at least signed-in 1,000 users – which prevents re-sessionising queries of users with rare characteristics, such as those using a rare language (because inferred language is covered by the metadata generalisation) or living in a sparsely populated area. This threshold is a lower bound – most end users will be in far larger groups. On top of that, signed-out users will be included in the groups, further increasing group size.

[1053] Annex 2 to Alphabet's response to the Preliminary Findings, Doc ID […], paragraph 33.

Finally, users can issue more than just one query, meaning that groups typically have far more than 1,000 queries in them (see recital (664)). A single query with a more granular location does not undo these anonymity groups – the query could still stem from any unique user within the group.

(744) Furthermore, Alphabet's results do not demonstrate direct re-identification risk stemming from these loose queries for which a more precise location is inferable. Alphabet indicates that within its sample of queries containing local intent, it was able to determine end user location with a median error of 2.9 km.[1054] Rather than quantifying actual risk, the examples that Alphabet presents are cherrypicked from a set of 700,000 queries, and the accuracy of the location was calculated using the true location of the user, which only Alphabet knows, and not an external attacker. Alphabet does not demonstrate how the accuracy of an inferred location could be verified without access to this ground truth. In addition, knowing the approximate location for one loose query in the format of "*restaurant near me*" is very unlikely to pose re-identification risk. Even Alphabet's cherrypicked examples do not illustrate such risk: Alphabet presents an example of someone searching "*gynecologist private near me*" and indicates that it was able to determine the location of the user within 1.3 km. However, within that radius, there is likely to be a significant amount of people that may be looking for a gynaecologist.

(745) The second result presented by Alphabet aims to demonstrate that auxiliary data from tracking cookies and network logs can be used to re-identify users. As a preliminary point, Alphabet's experiment does not take into account the contractual measures, which require a segregated data environment for the Search Dataset, separate from any auxiliary data, including advertising datasets. Furthermore, Alphabet limited the experiment by only counting users with "significant activity", which has been arbitrarily defined as users with at least 10 result clicks per week. This artificially inflates the numbers resulting from the experiment.

(746) Additionally, as set out previously, the information gain of such linking attacks is in most cases minimal. While the examples of URL linking shown by Alphabet cover sensitive topics, it is unclear what an attacker would learn from them. For example, it is not surprising that a query on how often a medicament can be used leads to a click on the URL of the producer's website, nor does it lead to re-identification risk.[1055] Accordingly, Alphabet's experiment does not call into question the Commission's assessment and conclusions set out in recitals (685) to (688).

(747) In conclusion, all examples of re-identification surfaced in Alphabet's testing either are effectively addressed in the specified measure in the present Decision or they do not bring the overall level of risk beyond residual level.

Summary of Commission's Anonymisation Testing Report

(748) The Commission worked with external experts to perform testing of the preliminary anonymisation measures, which has been made available to Alphabet in the Anonymisation Testing Report.

1054 Alphabet was able to confirm this figure because it has the ground truth on the end user's location, which an attacker would not have. Alphabet also presents an example where an exact user location can be determined from directions in Waze, a Google service. This result would be suppressed under the attribute suppression measures.

1055 See Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 78, bottom row of table. Alphabet only provided domains and not full URLs, meaning that the Commission cannot verify the experiments fully.

(749) The Anonymisation Testing Report's findings support that the specified anonymisation measures, as revised since the Preliminary findings, play a prominent role in mitigating the re-identification risk associated with the Search Data to a residual level. The report supports that the end user personal data that remains in queries after application of the technical anonymisation measures does not create a risk of end user re-identification that can be considered beyond residual level. The report also supports that re-sessionisation attacks are difficult to successfully and reliably perform at scale, especially in a way that enables meaningful information gain and that leads to successful re-identification.

(750) First, the Anonymisation Testing Report considers the risk associated with names in query text (the "**Commission's first experiment**"). Full names that pass the entity threshold and remain in the query text have been portrayed as an attack vector by Alphabet. The Anonymisation Testing Report finds that contrary to Alphabet's assertions, self-searches are exceedingly rare. This means that full names in the query text do not relate to the end user issuing the query – which is the scope of the anonymisation requirement – in the vast majority of cases. In a year, an average user is likely to search for [large number] to [large number] different names, meaning that an attacker that assumes a name in a query text relates to a self-searcher would be incorrect more than 99% of the time – rendering the associated risk below residual level.

(751) Manual analysis further confirmed that names in the query text are rarely enough to allow re-identification. Searches for names rarely include additional information that would either allow to deduce that the search is a self-search or provide meaningful information gain about the individual named in the query. This is especially true when considering the length threshold that limits the additional information that would fit in the query text.[1056] This further supports the conclusion that the risk associated with such queries can be considered residual.

(752) Second, the Anonymisation Testing Report considered addresses in the query text (the "**Commission's second experiment**"). The report found that overall, addresses in the query text are rare – the analysis identified addresses in only [0-10]% of the investigated sample of queries. Queries that did include an address in most cases did not include material additional information with the average address query only seven characters longer than the address. Queries that do contain additional information often exceed the length threshold. This shows that even in cases where the entity detection mechanism does not pick up on an address in a query text, the re-identification risk related to such queries is residual.[1057]

(753) Even when addresses are present, it is difficult to establish with certainty that the address relates to the end user who issued the query and not to another individual. As set out in recital (551), the scope of the anonymisation requirement of Article 6(11) of Regulation (EU) 2022/1925 extends only to the end user that issued the query. This effectively prevents large-scale re-identification of end users instrumentalising addresses in the query text.

(754) Third, the Anonymisation Testing Report considered the feasibility of re-sessionising queries (the "**Commission's third experiment**"). Alphabet argues that the technical anonymisation measures proposed in the Preliminary Findings leave the Search Data at risk of re-sessionisation.[1058] However, the Anonymisation Testing Report provides

---

1056 Anonymisation Testing Report, Doc ID […], Section 4.

1057 Anonymisation Testing Report, Doc ID […], Section 5.

1058 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 217-220.

quantitative evidence that re-sessionising queries is error-prone, uncertain, and would very rarely lead to an end user being re-identified and sensitive information being disclosed.

(755) The Anonymisation Testing Report attempted to re-sessionise queries within the same metadata bucket with the support of an LLM, focusing on the most re-identifiable and more sensitive query clusters. The Commission's third experiment showed that, despite a metadata group size far smaller than adopted in the measures, many query clusters that the LLM proposed were incorrect, meaning that the queries did not originate from the same user. The correct clusters were subsequently reviewed manually to determine whether they would cause material re-identification risk. The Commission's third experiment specifically targeted the most sensitive and re-identifiable sessions, and the qualitative analysis focused on the five most sensitive out of 30,000 potential sessions in the considered data. However, in the cases where clusters were correct (which a real-world attacker would have no means to verify), no cluster directly allowed end user re-identification. Even those with potentially re-identifying information would require significant work to confidently find out the identity of the end user. This suggests that such a task cannot be done on a large number of records in an automated manner.[1059]

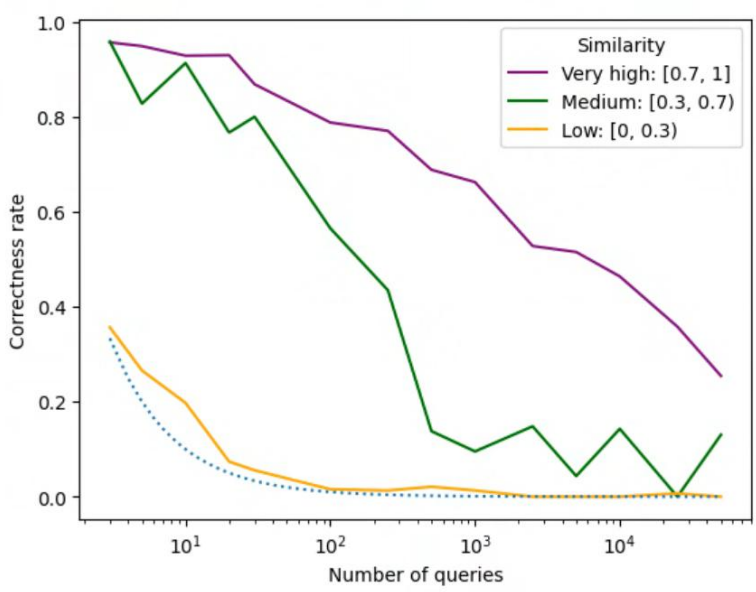
(756) Fourth, quantitative analysis of how often LLM-supported clustering succeeded in identifying user sessions with a metadata bucket (the "**Commission's fourth experiment**") confirms that re-sessionisation risk, especially of queries that are not highly similar, is negligible. This is an important factor, as re-sessionising dissimilar queries (i.e., queries that cover several different topics), is far more valuable to an attacker. It provides far more information gain about the end user, allowing the building of a richer profile, and making successful re-identification more likely. By contrast, re-sessionising two highly similar queries is unlikely to provide significantly more information than is present in either query in isolation. The Anonymisation Testing Report considered how two key parameters affect the feasibility of re-sessionising queries: (i) the similarity of the queries, and (ii) the metadata bucket size.

(757) As the results in Figure 15 show, the feasibility of such clustering quickly decreases as group size increases. This is because linking queries of the same user together becomes harder in a group that contains more different users. The Figure shows that even for queries that are about a similar topic (a similarity score between 0.3 and 0.7), the chance of being correct within a cluster of 1,000 queries is as low as 10%. For queries that are dissimilar (a similarity score under 0.3), the clustering success rate is close to a random guess (which is represented by the dotted line). Considering the similarity of queries is important, because real-world privacy risk from re-sessionisation would primarily stem from linking queries across topics together, giving an attacker significant information gain about an end user beyond one loose query and allowing the attacker to build a richer profile. This was the main issue around the 2006 AOL data release, which allowed linking queries across topics due to the pseudonymous nature of the data. In this dataset, attackers combined multiple unrelated queries from the same user: "*numb fingers*", "*60 single men*", "*dog that urinates on everything*", "*landscapers in Lilburn, Ga*", several people with the last name Arnold and "*homes sold in shadow lake subdivision gwinnett county*

[1059] Anonymisation Testing Report, Doc ID […], Section 6.

georgia."[1060] This is the kind of re-sessionisation that the results show is extremely hard to perform on the Search Dataset.

Figure 15: The rate at which query clusters were found to be correct (belong to the same end user) by group size and query similarity.



Source: Anonymisation Testing Report, Doc ID […], page 17.

(758) The group sizes in Figure 15 are expressed in queries, not unique signed-in end users. That means that in the technical anonymisation measures specified in the present Decision, which has at least 1,000 unique users in each metadata bucket, success rates will be even lower than the group sizes in the Figure suggest, as every user may issue multiple queries. Furthermore, 1,000 unique end users is a lower bound – most groups will have far more users in them (see recital (664)), making successful re-identification even more difficult.[1061]

Alphabet's observations on the Commission's testing

(759) Alphabet submitted observations on the Anonymisation Testing Report ("**Alphabet's Observations**" or "**Observations**").[1062] In these Observations, Alphabet argues that the Anonymisation Testing Report suffers from fundamental conceptual and methodological deficiencies.[1063] However, this is not the case.

(760) First, Alphabet presents the Anonymisation Testing Report as a narrow rebuttal of Alphabet's testing, instead of quantitative testing of re-identification risk. However, the Anonymisation Testing Report does both: (i) it quantitatively tests the likelihood of success of key attack vectors (names in queries, addresses in queries and re-sessionisation), and (ii) by doing so provides quantitative support that many of the examples raised in Alphabet's testing do not scale to a larger attack.

1060 See https://www.nytimes.com/2006/08/09/technology/a-face-is-exposed-for-aol-searcher-no-4417749.html, Doc ID […], last accessed on 24 June 2026.

1061 Anonymisation Testing Report, Doc ID […], Section 7.

1062 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […]. The additional re-identification risks presented in Section V of the report are addressed together with the remainder of Alphabet's testing results, cf. recital (721) et seq.

1063 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], Section III. Alphabet has not provided source code or detailed technical descriptions of its additional testing. Therefore, the Commission could not reproduce Alphabet's results.

(761) Second, contrary to what Alphabet asserts,[1064] the experiments carried out in the Anonymisation Testing Report are not artificially constrained. Alphabet claims that the experiments performed "ignore the ways that real attacks happen". But Alphabet does not specify which "real attacks" it is referring to. Alphabet's testing certainly does not mirror a "real attack". Alphabet's attack was performed by 10-15 engineers and did not have in place any of the technical, organisational and human controls prescribed in the contractual measures to ensure end users' anonymisation (see section 4.4.4.2.2) and protection of the integrity and confidentiality of the Search Data (see section 4.4.4.2.3).[1065] The right frame of reference is an attack that may be performed with the available time, cost, manpower and technology of an adversary on a dataset for which distribution is strictly controlled. The Expert Report on Anonymisation documents the assumptions on what can be considered a realistic attack; this was used as a starting point for the Anonymisation Testing Report. By contrast, Alphabet never seems to have conducted an analysis on which kind of attacks are realistic in the specific circumstances of Search Data sharing under Article 6(11) of Regulation (EU) 2022/1925 and did not take any adversarial assumptions into account when performing their testing.

(762) Third, Alphabet's claim[1066] that the experiments of the Anonymisation Testing Report suffer from sampling biases is equally misplaced. Alphabet presents the experiments, which aim to quantify risk of the overall dataset (e.g., out of 100 names, how many may be self-searches?) to a worst-case attack – the type of attacks that Alphabet's testing does. The fact is that the uniform sampling used in the report allows to generalise findings to the dataset and get an estimate of overall risk. Alphabet's worst-case testing cannot be generalised to the dataset because its examples are carefully selected among many records. By contrast, the approach taken in the Commission's experiments, i.e., evaluating the risk associated with a random record, is a meaningful way to evaluate the risk from attacks by insiders – an important type of possible attacker.[1067] For example, an employee trying to spy on their spouse cannot determine how many searches their spouse made, nor about what. From this attacker's perspective, their spouse *is* a random user in the data, and the Commission's experiments show that a targeted attack trying to re-identify this end user is highly unlikely to succeed.

(763) Fourth, contrary to Alphabet's claims,[1068] the Anonymisation Testing Report also does not dismiss examples of potential re-identification risk without justification. Instead, it considered the examples from an end-to-end re-identification standpoint applying the guiding principles set out in recital (619) above. Based on this analysis, the Anonymisation Testing Report concludes that none of the examples it identified is indicative of risk going beyond residual level.

(764) Alphabet's Observations next cover alleged issues with each of the four experiments in the Anonymisation Testing Report. In summary, Alphabet's arguments try to misrepresent the broader purpose of the experiment by pointing out narrow caveats. Alphabet does not demonstrate that the combination of measures fail at bringing re-

---

1064 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 13.

1065 Many of Alphabet's attacks rely on LLM inference. These attacks at scale would require LLM inference over billions of records – which would be a costly endeavour.

1066 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraphs 14-18.

1067 See Expert Report on Anonymisation, Doc ID […], sections 4.3.1 and 4.3.2.

1068 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 13.

identification risk down to a residual level. To establish risk of real-world harm beyond a residual level, the full chain of measures must fail:

(a) If the attack relies on query text, the attacker must extract sufficient context from this text to learn something about that person with sufficient certainty. It is hard to establish who issued a query – even about a sensitive topic. Query text is therefore not like a patient file with a diagnostic in it, which is certain to relate to the person named in the file. By contrast, end users can search for topics or conditions that concern other people, for example for a research project. Furthermore, a query that contains potentially identifying information (e.g., related to a rare disease) only enables re-identification if the attacker somehow acquires information about who has this rare disease. If this is known to the attacker, the query is unlikely to offer material additional information.

(b) If the attack relies on re-sessionisation, then the attacker must be able to re-sessionise queries together with high enough certainty and the queries must provide additional information for the attack to be worthwhile. Re-sessionising two identical or close-to-identical queries is unlikely to be useful.

(c) If the attack relies on increasing the granularity of location information, then the attacker must infer that information (e.g., via the query text or results). This is only possible for some queries within each large metadata bucket. Furthermore, such inference would only allow to gain a more precise location on loose queries. Gaining additional information requires re-sessionising the queries which is difficult, and if based on location, requires the target end user to stay in one place for it to work.

(d) If re-sessionisation relies on interaction data, then the attacker needs to gain sufficient certainty that interaction data is stable enough. In case the interaction characteristics differ per query or depending on the result, interaction data offers little basis for linking queries.

(e) Finally, the contractual measures need to fail for this to happen in practice.

(765) The Commission's first experiment, as set out above, shows that it is hard to determine whether a name is a self-search due to the large amount of name searches that take place. On the Commission's first experiment, which concerns names in the query text, Alphabet argues several deficiencies.[1069] However, none of the alleged deficiencies hold:

(a) Alphabet argues that the Commission's first experiment treats all names the same, rather than focusing on sub-groups (e.g., by filtering out celebrity names). However, the findings in the Anonymisation Testing Report stand even if an attacker were to apply this filtering. There is no clear distinction between celebrities and non-celebrities – instead the distribution is continuous and contains many "in-between" names that do not belong to well-known celebrities, but are local professionals, teachers, journalists, and so on. Reducing candidate names by filtering would take significant work considering the scope of data and the scope of names to be filtered out, and there is no clear definition that one could apply to define a celebrity. In any event, while such filtering would reduce the pool of names that may include self-searches, what remains would still be a massive corpus of queries including many names, of which only few are self-searches. Practically, the filtering suggested by

1069 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 24.

Alphabet could not be performed by the Commission due to shortcomings in Alphabet's platform, which does not allow internet access.

(b) Alphabet argues that the assumptions taken in the Anonymisation Testing Report are wrongly labelled as "conservative", by pointing out that metadata is not considered. This takes the Anonymisation Testing Report out of context: the report describes in which respects its assumptions are conservative, rather than just claiming the assumptions are conservative across the board. The fact remains that the assumption that every user that searched for a name searched for themselves at least once is very conservative – and even disproven.[1070] Furthermore, Alphabet simply asserts that metadata can be used to confirm whether something is a self-search but does not provide any evidence of this. For metadata to undermine the findings of the report, it would have to be done at a scale that significantly narrows down the overall corpus of queries with names to enable attackers to identify self-searches with high certainty – this is unlikely to be the case.

(c) Alphabet argues that the Anonymisation Testing Report's extrapolation to one year is baseless. This is not the case: this corresponds to the volume of data to which recipients will have access under the allowed retention period. Furthermore, it gives an indication of how frequent name searches are. Alphabet's claims that the daily data releases create immediate risk if an end user searches for three names on a given day. However, as the Commission's first experiment sets out: if an attacker cannot know whether the name belongs to the end user, there is no immediate risk. Alphabet further argues that a user may search for a name multiple times, and that this makes extrapolation inappropriate. This is fully misplaced – the repeated names would still be new data, and an attacker has no way of knowing whether these repeated searches were done by the same end user, meaning that they are not an indicator of a self-search.

(766) Alphabet purports to have performed testing which contradicts the Commission's first experiment's finding that self-searches are rare. However, the examples presented by Alphabet say little about how common self-searches are and for several examples, it is unclear whether the query even is a self-search.[1071] This, uncertainty among carefully picked examples demonstrates that it is challenging to ascertain whether something is a self-search:

(a) One query concerns an author with more than 11,000 followers on a topic that the author talked about publicly. This makes the assertion that it is a self-search extremely doubtful. The fact that Alphabet thought that this was a self-search based on the query text, even though a follow-up search shows that this is clearly related to a public figure, is a clear example for why it is, in general, very difficult to determine with high confidence whether a query containing a name is a self-search.

(b) Another query is a genealogy query and contains two names. Even if this were a self-search, this makes it inherently unclear which end user issued the query. Furthermore, there is no evidence that this is a self-search. While genealogy

---

1070 Research quoted by Alphabet in footnote 4 of Alphabet's Observations on the Hiding Nemo Report (Doc ID […]), dated 17 June 2026 finds that only about half of internet users have used an online search engine to look up their own name.

1071 Alphabet's phrasing suggests that it has not applied entity detection and query thresholding to filter out names that were queried less than 50 times before conducting its experiments.

queries may be likely to come from someone related to the names present in the queries, determining who issued the query remains far from straightforward.

(c) Alphabet also presents examples of queries about arrests and asserts that these are likely done by the end user. Alphabet does not provide evidence for this assertion – there are many people that may have reason to look up someone else's arrest.

(767) Alphabet's Observations additionally presents examples of users that query a full name, date of birth, and place of birth to determine their tax ID, which is readily computed based on those three data points for the jurisdiction in question. Alphabet indicates that it ran an LLM over 60,000 queries, to identify just over 100 queries for which the provided information allowed computing the tax ID. However, Alphabet does not clarify whether it confirmed that the queries in question would have passed the query suppression measures. Alphabet goes on to linearly extrapolate the 100 queries it found over a full year of data – despite its criticism on this practice set out in recital (765)(c).[1072]

(768) Alphabet's Observations finally presents examples of translation queries which contain data that is likely to belong to the end user – one shows an email address, and the other seems to include the password to a social media account. However, the email address presented is not a valid email address, and something that may be a password is not useful to an attacker without additional context – nor can it be used for re-identification.

(769) If Alphabet truly wanted to quantify how common self-searches are, it would have a very straightforward way of doing so: using the Google account information for signed-in users, which has the ground truth on users' names. The fact that Alphabet has not done so (or has chosen not to share the results of this analysis) is telling.

(770) The Commission's second experiment shows that addresses in queries are rare, and queries with addresses which include additional information that allow re-identification and pass the query suppression measures are even rarer. On the second experiment, Alphabet argues that the experiment suffered from deficiencies. However, these deficiencies do not hold:

(a) Alphabet claims that the street address detector used may have false negatives or miss location information that is less precise than a full address, and that therefore, any conclusion on the rareness of addresses is not fully conclusive.[1073] The Commission's second experiment does not purport to be fully conclusive on the rarity of precise location information (which is potentially most sensitive). The possibility that the detector may have missed some false negatives does not invalidate this conclusion. Alphabet has not demonstrated that the detector misses a meaningful amount of location information and misspellings that may get past automatic detectors would be far harder to find for attackers too.

(b) Alphabet claims that the detector used in the Commission's second experiment may be defective, as it did not find queries with more than one address in them

---

1072 Linear extrapolation is likely inappropriate for this example: interest in tax matters is highly seasonal and can be expected to coincide with when tax filings are due. The risk from such queries is therefore significantly overstated.

1073 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraphs 30a and 30d.

in the sample investigated.[1074] However, Alphabet does nothing to support this assertion, despite having received the source code of the experiments, which allows it to reproduce the findings. As set out above, Alphabet has not provided source code supporting its own report with observations.

(c) Alphabet calls into question the Commission's second experiment's finding that queries are on average only seven characters longer than the address itself – claiming that as most queries only contain an address without additional information, a small number of queries must contain significant additional information.[1075] However, considering the length threshold applied to queries as part of the query suppression, many of these queries with material additional information do not pass the length threshold and would be suppressed.[1076]

(771) Alphabet also argues in its Observations that addresses in query text are not low risk and that a significant number of queries contain addresses as well as supplementary information. However, Alphabet's analysis does not support this conclusion. Alphabet investigated a week of EEA data but appears not to have applied the entity threshold to that data, meaning it did not confirm whether addresses it found pass the threshold of 50. Despite this, Alphabet only identified around 2,400 queries containing a name and an exact address in a week of EEA data.[1077] Considering the scale of the data, this means such queries are exceedingly rare. It shows that a random record would almost certainly not contain an address, and an attacker targeting a specific person would almost certainly not be able to learn their address from the data or use their address for re-identification. There is also no indication of which proportion of addresses are real and private – they could be doctor's offices, or another publicly available address. There is also no indication that the name and address belong to the end user – which is the scope of the anonymisation requirement. Finally, it is not clear why an attacker would go through the trouble of isolating addresses in this dataset at scale. The information gain of such an attack, which would be costly to perform,[1078] is likely minimal: the resulting data would be an assortment of unstructured, potentially-wrong addresses' data of random people, largely without any additional information.

(772) The Commission's third experiment shows that it would be difficult for an attacker to confidently re-sessionise queries belonging to the same user, and that where this is successful, it often does not lead to enough information to re-identify the end user. On the Commission's third experiment, Alphabet claims to have identified several deficiencies, but none of these hold:

1074 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 30b. Alphabet further argues that the sampling method may be defective. However, the sample size was constrained by the technical limitation of the platform made available by Alphabet.

1075 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 30c.

1076 As set out in recital (650), the length threshold is approximately [50-75] characters for English. Alphabet argues that as [Alphabet's internal figure] out of 100 queries do not contain any information beyond an address, the remaining [Alphabet's internal figure] queries must contain a significant amount to bring the average to [number of characters] characters. Taking those numbers, the average number of additional characters in the [Alphabet's internal figure] queries in question is [number of characters] characters – this is very unlikely to leave sufficient space for an address and yet remain under the length threshold of [50-75] characters.

1077 Alphabet extrapolates this to 125,000 queries across the EEA per year, despite previously criticising linear extrapolation in the same submission – see Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 24.

1078 Isolating the addresses from the EEA data would require running the entire dataset through personal data detectors.

(a) Alphabet argues that the experiment is constrained by ignoring auxiliary data. This misses the point of the experiment. The experiment investigates the most sensitive re-sessionisation cases – and how confident an attacker could be to find queries belonging to the same user. Linking based on auxiliary data is a different type of attack, which is in any case addressed by the measures.[1079]

(b) Alphabet criticises the scope of the experiment for focusing on English-language queries and same-day re-sessionisation. However, Alphabet does not provide any reason to support the assertion that this invalidates the argument. There is no reason to believe that data from different days is easier to re-sessionise. On the contrary: considering multiple days increases the bucket size, mathematically making re-sessionising across days harder. Furthermore, the experiment focusing on English language is simply a result of the data made available by Alphabet for testing, which is a week of Irish data – a predominantly English-speaking country.[1080]

(c) Alphabet criticises that the experiment's LLM prompt asked the LLM to both cluster queries and identify queries that are more sensitive, arguing this affected the effectiveness of the LLM clustering. Alphabet does not support this assertion with evidence or support its assertion that this is unlikely to mirror the approach taken by an attacker. The experiment focused on the worst-case risk for re-identification of end users through re-sessionisation and was not limited to the possibility of re-sessionising only – which is evaluated in the Commission's fourth experiment.

(d) Alphabet criticises that the experiment only evaluates clusters that are fully correct (i.e., all queries belong to the same user), and claims that clusters that contain some incorrect queries can be harmful too. However, this again misrepresents the objective and findings of the experiment. The experiment assessed a worst-case scenario, namely clusters that are fully correct and marked as the most sensitive by the LLM. These were manually reviewed to establish the re-identification risk. It is valid not looking at partly incorrect queries as part of this worst-case analysis – the incorrect queries introduce additional uncertainty, which support the findings of the experiment.

(e) Alphabet also disputes the experiment's finding that even for the correct clusters that were manually evaluated, it is hard to re-identify an end user based on these clusters. Alphabet asserts that the risk in relation to these queries cannot be considered insignificant. However, this misrepresents the Commission's anonymisation approach. The approach relies on a combination of technical measures and contractual measures to reduce re-identification risk to insignificant. When looking at technical measures in isolation, a level of residual risk may remain – this is what the experiment assessed.

(773) The Commission's fourth experiment shows that re-sessionising queries in larger metadata buckets is difficult, particularly for queries that cover different topics, which would be the most valuable sessions for attackers as they allow them to build a

1079 See recitals (685) - (691).

1080 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraph 40a. Alphabet additionally criticises the remaining limitations which are outlined in the report, such as the capabilities of the LLM used. These limitations are driven by constraints of the testing environment made available by Alphabet.

richer profile of an end user. Alphabet claims that the fourth experiment shows deficiencies, but that is incorrect:[1081]

(a) Alphabet claims that the report baselessly assumes that closely related queries do not pose a privacy risk. This is not the case. The report considers that there is a spectrum: re-sessionising identical queries is largely pointless, and re-sessionising very different queries is on average more problematic as these may contain new information that could be used to re-identify an end user or build a richer profile of them. Closely related queries are on the less risky side of that spectrum. As set out in section 4.4.1, some residual level risk remains after application of the technical measures. It is the combination of technical measures and contractual measures that reduces risk to insignificant level.[1082]

(b) Alphabet again claims that limiting the scope of the experiment to a single day and English language queries is a deficiency. This is not the case, as laid out in recital (772)(b).

(c) Alphabet argues that it is inappropriate to use an LLM to measure query similarity, and that having the same LLM assess query similarity and clustering introduces biases. Alphabet does not provide any evidence for this claim. Furthermore, the experiment was designed under the limitations of the testing platform made available by Alphabet, which did not have technologies such as embeddings or different LLMs available.

(d) Alphabet argues that the experiment does not perform a re-sessionisation attack under realistic conditions, and that in reality, a re-sessionisation attack is performed iteratively. Alphabet does not provide evidence for this claim, and evidence suggests that re-sessionising does not get easier the more queries one has. In fact, it becomes harder. This explains why Alphabet used a threshold of only two queries for its own re-sessionisation experiments.

(774) On the Commission's third and fourth experiment, Alphabet presents alternative testing evidence which according to Alphabet's Observations invalidate the experiments' conclusions.[1083] However, the findings of Alphabet's alternative testing do not contradict the findings in the Anonymisation Testing Report. Contrary to Alphabet's assertions, the Anonymisation Testing Report does not claim that attackers will never be able to re-sessionise queries. Instead, the Commission's third and fourth experiments have different objectives:

(a) The Commission's third experiment assesses the re-identification risk of the most sensitive sessions – something that Alphabet's alternative testing does not do. While Alphabet's alternative testing cherry picks sessions on sensitive topics, it does not demonstrate the re-identification risk stemming from them, which is the focus of the Commission's third experiment. Furthermore, the

---

1081 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraphs 51-52. In paragraph 51, Alphabet points out that the success rate for very high similarity queries at group size 5,000 is approximately 50%, not 20% as stated in the report. This is a clerical error in the report, which intended to refer to bucket size 50,000 (the end of the axis of the graph), where the success rate approaches 20%. This clerical error does not affect the report's findings.

1082 Alphabet additionally claims that re-sessionising very close queries could reveal information about user behaviour and metadata. However, it is not clear how, considering that all re-sessionisation examples presented in Alphabet's observations use queries from the same metadata bucket.

1083 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraphs 43-46. It is unclear from Alphabet's description whether it exclusively worked with metadata buckets of 1,000, or the metadata buckets that would result from applying the technical message, which are far larger on average (1,000 is a lower bound, see recital (664)).

examples surfaced by Alphabet all concern highly similar queries, meaning that an attacker would gain limited information compared to each query individually.

(b) The Commission's fourth experiment gives an assessment of re-sessionisation risk – considering bucket size and query similarity – that can be generalised across the dataset and therefore gives a representative quantification of the risk. Alphabet's testing, which focuses on worst-case examples only, does not give such quantitative assessment of re-sessionisation risk.

(775) The high similarity of queries within the clusters that Alphabet's alternative testing found, are explained by the design of its test – which seems optimised to find a high success rate, rather than clusters that present real-life re-identification risk. Alphabet uses an LLM to propose clusters of queries based on semantic similarity and click signatures. It then uses a measure of text similarity, the Jaccard index, to prune queries from the clusters that are textually dissimilar from other queries in the cluster. While this increases the chance that a cluster is correct (i.e., consists of queries by the same user), it also makes the cluster far less practically useful. By design, all queries in the cluster will be highly similar, making it unlikely that the clusters cover different topics.

(776) The examples presented by Alphabet's alternative testing confirm this and thereby support the findings in the Anonymisation Testing Report. Alphabet does not show examples of re-sessionising queries across different topics, which pose the most material privacy risk. The examples shown by Alphabet, which consist of similar queries, show that such re-sessionisation often does not lead to a material amount of additional information. Often, a single query in the group gives close to all there is to learn from the overall session.[1084] For each of the examples, the attacker must know the identified information about their target to begin with to re-identify the target successfully – in which case re-sessionisation does not meaningfully help them. The examples provided by Alphabet's alternative testing are therefore very far from confirmed re-identification.

4.4.4.1.2.1.8. Conclusion

(777) The technical anonymisation measures combine the removal of attributes, query suppression, metadata generalisation and mini-sessionisation. Together, these technical measures effectively reduce the risk of end-user re-identification to a residual level, thereby playing a prominent role in ensuring end users' anonymisation, while the complementing contractual measures set out in section 4.4.4.2. further contribute to meeting that requirement by addressing the remaining residual risk associated with the sharing of Search Data under Article 6(11) of Regulation (EU) 2022/1925.

(778) **First**, the Commission reduces the risk of attackers singling out end users and grouping their queries by suppressing end-user identifying attributes, such as account identifiers and timestamps. This turns the dataset into a haystack of loose queries, with the exception of mini-sessions consisting of at most three highly related queries. This makes it significantly more difficult for attackers to single out individual end users and strongly limits the information gain of attacks. Furthermore, the Commission specifies query suppression to remove identifiers in the query text and

[1084] For example, one set of queries concerns a military spouse trying to open a U.S. checking account. The queries all convey highly similar information, and it is not clear how they can be a basis for re-identification. Another concerns chlamydia treatment – all queries are highly similar and do not contain further information on the end user.

metadata generalisation to achieve indistinguishability among groups of end users, thereby mitigating the risk of singling out.

(779) **Second**, the Commission mitigates the risk of inferring new information about an identifiable end user by suppressing user account identifiers and other attributes in the search record and removing identifiers in the query text with query suppression that could be used to identify the end user of whom information may be inferred. Additionally, metadata generalisation coarsens location, resulting in indistinguishability amongst end users from a metadata perspective, which prevents inferring information about an identifiable end user.

(780) **Third**, the Commission mitigates the risk of linking by suppressing end-user identifying attributes, such as timestamps and IP addresses, that an attacker could link to auxiliary datasets. Query suppression removes identifiers from the query text that an attacker could use for linking purposes as well, and metadata generalisation coarsens location, making it more difficult for attackers to link search records to external datasets or their own contextual private knowledge. Additionally, suppression of direct identifiers makes additional information gain from such attacks unlikely, as the linking would only affect one individual query.

(781) Contrary to Alphabet's submission, the Commission has not merely asserted that the specified technical measures reduce re-identification risks to a residual level without substantiating that conclusion.[1085] Instead, the Commission's assessment is supported by the Expert Report on Anonymisation, a structured risk assessment set out in recital (619), adopts well-established practices such as *k*-anonymity, and by empirical testing carried out by the Commission on a sample of the Search Data directly relevant to the criteria set out in that risk assessment (section 4.4.4.1.2.1.7) as well as by the Commission's detailed assessment of several rounds of testing carried out by Alphabet (see section 4.4.4.1.2.1.7). On that basis, the Commission has established, by reference to objective criteria and sufficient evidence, that the specified technical measures reduce the risks of re-identification from singling out, linking and inference and that the remaining overall risk of end users' re-identification after application of the specified technical measures is not beyond residual level in accordance with the risk assessment set out in recital (619). The Commission has therefore demonstrated that the technical measures, together, play a prominent role in ensuring end users' anonymisation.

4.4.4.1.2.2. The Commission's technical measures maintain a higher level of data quality and usefulness than Alphabet's current anonymisation approach

(782) The Commission considers that the technical measures achieve a higher level of data quality and usefulness for the purpose of optimising the services of third-party online search engines than Alphabet's current approach does, while reducing the risk of re-identification to a residual level.

(783) **First**, the technical measures share Search Data at the record-level, as opposed to an aggregated level. The effectiveness of online search engines relies heavily on algorithms that are trained on diverse individual records, and consequently, releasing aggregated data and statistics instead would dramatically reduce the quality and usefulness of the Search Data. Virtually all potential beneficiaries agree that aggregated data is significantly less useful than record-level data as it lacks the

[1085] Alphabet's response to the Alphabet's response to the Revised Measures, Doc ID […], paragraphs 24-33.

required granularity to effectively improve their online search engines.[1086] (see also recital (385) on the importance of record-level data).

(784) **Second**, the data quality cost of the word-based threshold is significantly smaller than Alphabet's query suppression proposal, even when using large *w*-threshold values. For example, using an entity-based threshold of $w = 50$ removes approximately [10-20]% of unique queries, and a threshold of $w = 100$ removes approximately [10-20]% of unique queries[1087]. In contrast, Alphabet's threshold of 30 applied to the full query removes approximately [90-100]% of unique queries (in the absence of the allow list).[1088]

(785) **Third**, while the Commission's metadata generalisation uses a threshold of 1,000, which is higher than Alphabet's *m*-threshold, the Commission's metadata generalisation does not apply to the query text. A large proportion of the excluded data is likely driven by applying the threshold to the query text as well, as that field can take a large variety of values. The Commission's approach is therefore likely to maintain a higher level of data quality and usefulness than Alphabet's approach.

(786) **Fourth**, while Alphabet's approach does not provide any session-level data, the Commission's technical measures release limited session data in the form of mini-sessions. Session data conveys valuable information about query intent, as end users frequently reformulate queries to refine the results to their liking. In this regard, one third party explains that such data is useful for understanding "*query similarity, query rewriting, intent classification (assessing the final website visited by user), ranking along the session by assessing the real information the visitor was looking for from the last website visited, switching the paradigm from answering a query and optimising for getting a click on rank 1 to answering user need directly from 1st query in the session*".[1089]Another third party states: "*Sessions and reformulation data are an essential part for optimising the relevance of a search engine's results. This could take the form of several Queries and their associated Rankings, View, and Click data that have been performed by the same user within a certain time window.*"[1090] Another third party explains: "*sessions can be used to better understand query refinement, measure user satisfaction signals, evaluate ranking and retrieval changes, reduce repeated effort in serving related queries, and improve features such as query suggestions and spelling correction.*"[1091]

(787) **Fifth,** while Alphabet's approach only releases data quarterly and provides no more detailed timestamp data, the Commission's approach releases data daily. Operators of OSEs explain that frequent release of the Search Data and granular timestamp data are important for the optimisation of their services. For instance, one third party explains "*[t]emporal context is important to understand freshness and relevance, particularly for news and time-sensitive queries"*.[1092] It is also important that data is fresh and not shared with significant latency. This is confirmed by virtually all

---

1086 See, for example, [market participants]on Compliance with Article 6(11), DMA (Click-and-Query Data), Doc ID […], and [Market participant]'s Comments on Google's Digital Markets Act Article 6(11) Compliance Proposal, Doc […].

1087 Alphabet's reply to RFI 16 of 22 May 2025, Doc ID […], question 1.

1088 Alphabet's reply to RFI 11 of 12 November 2025, Doc ID […], question 7. Alphabet performed the analysis over 10 months of search data, rather than 13 months. However, the results unlikely to change materially when considering 13 months.

1089 [Market participant]'s reply to RFI 2 of 12 February 2026, Doc ID […], question 4.

1090 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 3.

1091 [Market participant]'s reply to RFI 2 dated 12 February 2026, Doc ID […], question 4.

1092 [Market participant]'s reply to RFI 1 of 28 January 2026, Annex 1 (Doc ID […]).

market participants.[1093] One market participant explains that when relying on old Search Data, crawling priorities will be inaccurate, the relevance for queries declines and it is more difficult to implement changes in the SERP layout.[1094] (see also section 4.3.3.2 on the importance of timestamp data and frequency of sharing).

(788) **Sixth**, while Alphabet's approach only releases location data on country granularity, regardless of the size of the country, the Commission's measures use an adaptive approach that is based on NUTS3 regions. NUTS3 regions have roughly similar populations (between 150,000 and 800,000), meaning that the location data provided under the Commission's approach is far more granular – particularly for larger countries.

4.4.4.2. Contractual measures

(789) The Commission specifies contractual measures in relation to anonymisation that Alphabet must implement to comply effectively with Article 6(11) of Regulation (EU) 2022/1925. As set out in section 4.4.1, the contractual measures mitigate the residual likelihood of identification that remains after applying the technical measures to Search Data (referred to hereafter as the "Search Dataset") so as to ensure that such likelihood is, from the perspective of third-party OSEs[1095] or any third other person,[1096] insignificant, taking into account all means reasonably likely to be used to identify end users.

(790) Since the sharing of or granting access to the Search Dataset, insofar as it will include personal data of other individuals than end users, is a processing of personal data subject to Regulation (EU) 2016/679, the Commission considers that the contractual arrangements between Alphabet and third-party OSEs should reflect an appropriate allocation of roles and responsibilities between the parties to ensure effective compliance with Article 6(11) of Regulation (EU) 2022/1925 while ensuring appropriate protection of the Search Dataset and compliance with applicable rules of Regulation (EU) 2016/679 (section 4.4.4.2.1).

(791) The Commission further considers that, in order to mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk, Alphabet should impose on third-party OSEs the following set of contractual obligations which, taken together and in combination with the technical measures, ensure anonymisation of end users' data and thereby the effective implementation of Article 6(11) of regulation (EU) 2022/1925:

(a) contractual obligations to ensure anonymisation from the perspective of the third-party OSE recipients (section 4.4.4.2.2);

(b) contractual obligations to protect the integrity and confidentiality of the Search Dataset to ensure anonymisation against any third other person (section 4.4.4.2.3); and

(c) an independent verification mechanism to ensure the auditability and verifiability of anonymisation over time (section 4.4.4.2.4)

1093 Responses to RFI 1 of 18 November 2025 by [market participant] (Doc ID […]), [market participant](Doc ID […]), [market participant](Doc ID […]), [market participant] (Doc ID […]), [market participant](Doc ID […]) and [market participant](Doc ID […]).

1094 [Market participant]'s reply to RFI 1 of 18 November 2025, Doc ID […], question 11.

1095 Throughout this section (613), the 'third-party online search engines' refers to the third-party undertakings providing online search engines and the third parties with whom they have contracted in order to process Search Data on their behalf as processors and any sub-processors (i.e. subcontractors).

1096 Any other person does not include Alphabet as it is always in a position and capacity to re-identify its own end users.

4.4.4.2.1. Roles and responsibilities in the sharing and processing of the Search Dataset

(792) The Commission considers that to ensure effective compliance with Article 6(11) of Regulation (EU) 2022/1925, in particular to ensure access on FRAND terms, the contractual arrangements between Alphabet and third-party OSEs should reflect an appropriate allocation of roles and responsibilities between the parties, while ensuring appropriate protection of the Search Dataset in compliance with applicable rules of Regulation (EU) 2016/679.

4.4.4.2.1.1. Measures

(793) The Commission considers that the following measures are required to specify how Alphabet must comply with its obligation under Article 6(11) of Regulation (EU) 2022/1925.

(794) Alphabet must ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, that Alphabet and the third-party OSE are recognised as independent controllers within the meaning of Article 4, paragraph 7 of Regulation (EU) 2016/679.

(795) Alphabet must ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, the following allocation of responsibilities:

(a) Alphabet is controller for the processing of end users' personal data carried out to implement the technical measures set out in section 4.4.4.1 prior to the sharing or granting access to the Search Dataset;

(b) Alphabet ensures that the sharing or granting access to the Search Dataset is carried out in a secure manner, in accordance with Articles 5(1)(f) and 32 of Regulation (EU) 2016/679 and, where applicable, in compliance with the requirements of Chapter V of that Regulation;

(c) The third-party OSE accessing the Search Dataset is responsible and liable for ensuring the lawful and compliant processing of personal data of individuals other than end users forming part of the Search Dataset under Regulation (EU) 2016/679, including any processing performed by third parties with whom it has contracted to process the Search Dataset on its behalf acting as processors or authorised sub-processors (i.e. subcontractors).

(d) The third-party OSE accessing the Search Dataset is responsible to ensure that any subcontractors involved in the processing of the Search Dataset are contractually bound to implement all relevant contractual measures set out in sections 4.4.4.2.2.1 and 4.4.4.2.3.1, and that contractual arrangements with such subcontractors explicitly provide independent auditor(s) with the right to verify compliance with these contractual measures in line with the measures in section 4.4.4.2.4.1;

(e) The third-party OSE is responsible and liable under Regulation (EU) 2016/679 for any personal data processing resulting from a breach or circumvention of the contractual measures imposed by Alphabet to ensure anonymisation of end users' personal data, including any processing performed by subcontractors, without prejudice to the allocation of responsibility and liability under that Regulation, in particular Articles 82 and 83 thereof.

(796) Alphabet must ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, that it imposes only the contractual measures complementing the technical measures necessary to ensure anonymisation of the

Search Dataset set out in sections 4.4.4.2.2.1, 4.4.4.2.3.1 and 4.4.4.2.4.1, without extending control over the third-party OSE's independent processing activities.

4.4.4.2.1.2. The Commission's assessment

(797) As explained in recital (551) of this Decision, Regulation (EU) 2016/679 applies to the sharing or granting access to the Search Dataset by Alphabet and to the re-use of the Search Dataset by third-party OSEs. This is so because the anonymisation requirement is limited, in accordance with the legislator's intent, to the protection of *end users'* personal data against possible re-identification risks, but does not extend to personal data of other individuals which is collected, retrieved, indexed and as the case may be, disclosed and made available to end users in search results and which form an integral part of the OSE activity.[1097] The Search Dataset inevitably includes personal data relating to individuals other than end users, and Article 6(11) of Regulation (EU) 2022/1925 mandates the sharing or granting of access to those personal data by the gatekeeper, as such sharing is necessary, within the meaning of Articles 6(1)(c) and 9(2)(g) of Regulation (EU) 2016/679, to preserve the level of data quality and usefulness for third-party OSEs, thereby contributing to the effective achievement of the contestability objective pursued by that provision. That contestability objective constitutes a substantial public interest recognised by Regulation (EU) 2022/1925 within the meaning of Article 9(2)(g) of Regulation (EU) 2016/679.

(798) At the outset, Alphabet's claim that the fact described above (i.e. that the Search Dataset inevitably include personal data relating to individuals other than end users) would amount to an acknowledgement by the Commission that "*user data remains personal data as it cannot be possible for user data to be anonymised but for non-user data to remain personal data*"[1098] mischaracterises both the Commission's reasoning and the concept of personal data under EU data protection law. Alphabet incorrectly assumes that anonymisation must operate uniformly across all possible categories of data subjects represented in a dataset such as the Search Dataset.

(799) However, it is well-established that the same information can, under EU data protection law, simultaneously relate to multiple data subjects.[1099] This is also true for Search Data, which can simultaneously relate to the end users who generated the queries and to other individuals (e.g. famous people, professionals or other) who are the subject of queries and whose personal data may be processed, indexed, retrieved and made available to end users. Since the scope of the anonymisation requirement is limited to end users' personal data and does not extent to other individuals, this means that Article 6(11) of Regulation (EU) 2022/1925 requires to assess identifiability in relation to end users only. Accordingly, this means that information may cease to permit identification of one category of data subject (i.e. end users) while remaining personal data in relation to another category of data subjects (i.e. other individuals). It follows that the fact that the Search Dataset inevitably contains personal data relating to individuals who are the object of queries neither preclude

---

1097 Judgment of the Court of Justice of 13 May 2014, *Google Spain SL, Google Inc. v AEPD*, C-131/12, ECLI:EU:C:2016:779, paragraph 27 to 29: "*It is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons, and thus 'personal data'*".

1098 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 300-301.

1099 See for instance judgment of the Court of Justice of 20 December 2017, Peter Nowak v Data Protection Commissioner, C-434/16, ECLI:EU:C:2017:994, paragraph 45: " The same information may relate to a number of individuals and may constitute for each of them, provided that those persons are identified or identifiable, personal data, within the meaning of Article 2(a) of Directive 95/46".

the anonymisation of personal data relating to the end users who generated those queries nor imply that the anonymisation measures applied to end-users' personal data are ineffective.

(800) Instead, the fact that the Search Dataset will inevitably contain personal data relating to other individuals than the end users necessarily entails the continued application of Regulation (EU) 2016/679 to the sharing of the Search Dataset and to the subsequent processing operations carried out by third-party OSEs. The continued application of Regulation (EU) 2016/679 is neither contradictory to nor incompatible with the anonymisation requirement enshrined in Article 6(11) of Regulation (EU) 2016/679, which scope is limited to end users' personal data. The EDPB also expressly supports that analysis.[1100] Far from being inconsistent, the continued application of Regulation (EU) 2016/679 provides continued protection to individual's personal data forming part of the Search Dataset other than end users' anonymised data.

(801) **First**, since Regulation (EU) 2016/679 applies to the sharing or granting access to the Search Dataset, the Commission considers that the effective implementation Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to ensure that contractual arrangements with third-party OSEs accessing the Search Dataset reflect an appropriate allocation of roles and responsibilities respecting their independent controllership[1101] with regard to the respective processing operations carried out under their control.

(802) In this regard, the Commission observes that Alphabet's Search Data agreement requires third-party OSEs to obtain Alphabet's prior express consent for each "authorised vendor", namely any third-party vendor or recipient engaged by the third-party OSE to process Search Data on their behalf to optimise its OSE, and to provide detailed information regarding such vendors, including a description of the applicable contractual terms.[1102] Alphabet claims that its Search Data Agreement and the particular clauses described in section 4.4.2.2 are necessary to ensure protection of Alphabet's commercially sensitive information.

(803) However, as explained in recital (551), the Commission considers that Alphabet's obligation under Article 6(11) of Regulation (EU) 2022/1925 read in the light of recital 61 concerns end-user generated data, that is "*ranking, query, click and view data in relation to free and paid search generated by consumers*", and does not extend to Alphabet's algorithms or other intellectual property. In any event, even if some specific data attributes forming part of the Search Dataset could ever be considered as commercially sensitive information, which is far from obvious, such information is in any way appropriately protected through the contractual measures provided for in sections 4.4.4.2.2.1 and 4.4.4.2.3.1 and the independent verification mechanism described in section 4.4.4.2.4.1.

(804) Article 6(11) of Regulation (EU) 2022/1925, read in conjunction with recital 61 thereof, provides that "*access should also be granted to third parties contracted by a provider of an online search engine who act as processors of such data on behalf of that online search engine*." The possibility for the third-party OSE, as controller, to

---

1100 EDPB comments on the proposed measures of 5 May 2026, Doc ID […], paragraph 1.

1101 Article 4(7) of Regulation (EU) 2016/679 defines 'controller' as "*the natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

1102 Google's Search Data agreement, Doc ID […], definition of "authorised vendor" in clauses 1.1 and clause 2.3.2.

rely on third parties with whom it has contracted to access and process Search Data *on its behalf* as processors (referred to in this Decision as "sub-contractors") would be significantly impeded if it were subject to Alphabet's approval of that processor, which is moreover not limited to specific grounds of refusal. Indeed, if the gatekeeper were permitted to exercise prior approval over the processors engaged by third-party OSEs, this could confer on the gatekeeper decisive influence over an essential means of processing and could in practice subordinate the processing chain of the Search Data to the gatekeeper's control.[1103] Accordingly, specifying that third-party OSEs are independent controllers contributes to implement Article 6(11) of Regulation (EU) 2022/1925 in a manner that ensures that the third-party OSE retains, as independent controller from Alphabet, the inherent autonomy over the essential means of processing, in particular the choice of its subcontractors involved in the processing of Search Data on its behalf.

(805) **Second**, as a result of the independent controllership of Alphabet and third-party OSEs, the Commission considers that responsibility must be logically allocated in a way that ensures that accountability for processing remains with the party exercising control.

(806) As regards Alphabet, it is the controller for the processing of end users' personal data necessary to implement the technical measures set out in section 4.4.4.1 prior to granting access to the Search Dataset. It is also responsible for ensuring that the granting of access to the Search Dataset to a third-party OSE is carried out in a secure manner and where applicable in the case of international transfers of the Search Dataset, in compliance with the requirements of Chapter V of Regulation (EU) 2016/679 (see section 4.2.4).

(807) As regards third-party OSEs, they are responsible and liable for the processing of personal data of individuals other than end users forming part of the Search Dataset under Regulation (EU) 2016/679.

(808) Given that access to the Search Dataset is granted for the purpose of optimisation and improvement of online search engine services (see below recital (822) and recitals (846) to (851)), and that this purpose will be pursued by the third-party OSE *in the management of its own business*, the third-party OSE acts as an independent controller (independent from Alphabet) in the processing of personal data for that purpose.[1104]

(809) As a separate controller, the third-party OSE is therefore responsible, among other obligations, to ensure that any processing carried out using the Search Dataset is based on an appropriate lawful ground under Article 6 of Regulation (EU) 2016/679, including where the Search Dataset is used for the training or fine-tuning of machine learning models, including models supporting ranking, retrieval, or AI chatbot functionalities.[1105] Third-party OSEs relying on Article 6(1)(f) of Regulation 2016/679[1106] are responsible for assessing and, where required, demonstrating to the

---

1103 EDPB Guidelines 07/2020, version 2.1, of 7 July 2021 on the concepts of controller and processor in the GDPR, Doc ID […], in particular see in Part I "Concepts", section 2.1.4 on "Purposes and means", section 4 on "Definition of processor" and in Part II "Consequences of attributing different roles", section 1.1 "Choice of processor", available at: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

1104 See by analogy the judgment in Case C-200/23 *Agentsia po vpisvaniyata* EU:C:2024:827, paragraphs 76 and 79.

1105 See EDPB comments on proposed measures of 5 May 2026, paragraph 12.

1106 Article 6(1)(f) of Regulation (EU) 2016/679: "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by*

competent supervisory authorities, that such processing is necessary for the legitimate interests pursued and that appropriate mitigating measures are implemented to ensure that the interests, rights and freedoms of the individuals concerned do not override those legitimate interests in accordance with relevant EDPB guidelines and opinions.[1107]

(810) In that context, as third-party OSEs must retain autonomy for the choice of their subcontractors, it is nevertheless their corresponding responsibility, as controllers, to ensure that those subcontractors acting as processors and sub-processors, where appropriate, will implement all relevant measures necessary for the third-party OSE to meet its contractual obligations towards Alphabet. If the third-party OSE fails to ensure implementation of all relevant measures, the third-party OSE would *de facto* not be in a position to meet its contractual obligations towards Alphabet. Third-party OSEs must therefore be responsible to ensure that subcontractors involved in the processing of the Search Dataset are contractually bound to implement all relevant contractual measures set out in this section 4.4.4.2, and that contractual arrangements with such subcontractors explicitly provide independent auditor(s) with the right to verify compliance with these contractual measures to ensure anonymisation of end users' data in accordance with the measures outlined in section 4.4.4.2.4.

(811) Where a breach or circumvention of the contractual measures imposed by Alphabet results in the processing of personal data, essentially because the end users' data forming part of the Search Dataset can no longer be considered as effectively anonymised, such processing would fall within the scope of Regulation (EU) 2016/679 and, in the absence of a valid ground under Article 6 and 9 of that Regulation, may give rise to responsibility and liability of the third-party OSE, including in relation to processing carried out by its subcontractors. As a result, the third-party OSEs will be responsible and liable under Regulation (EU) 2016/679 in such circumstances, without prejudice to the allocation of responsibility and liability under that Regulation, in particular Articles 82 and 83 thereof.[1108]

(812) In this regard, the Commission notes that undertakings providing OSEs services in the Union are already controllers for the processing of personal data carried out under their independent control when providing online search services to their own end users. It follows that allocating responsibility and liability under Regulation (EU) 2016/679 for any personal data processing resulting from a breach or circumvention of the contractual measures imposed by Alphabet cannot, in this context, be considered as an imbalance of obligations raising contradiction with Article 8(8) of Regulation (EU) 2022/1925.

(813) **Third**, the Commission considers that the effective implementation, through contractual arrangements, of its obligation to grant access to the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to impose only the contractual measures complementing the technical measures necessary to

---

the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

1107 EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR adopted on 8 October 2024, version 1.0 and EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models adopted on 17 December 2024, section 3.3.

1108 Articles 82 and 83 of Regulation (EU) 2016/679 grant individuals the right to compensation for damage caused by an infringement of the GDPR and set out the general conditions for imposing administrative fines. Under these provisions, responsibility towards the competent supervisory authorities and liability for compensation claims can be divided between the controller and its processor depending on their respective roles and the circumstances of the infringement or resulting damage.

ensure anonymisation of the Search Dataset set out in sections 4.4.4.2.2.1, 4.4.4.2.3.1 and 4.4.4.2.4.1, without extending control over the third-party OSE's independent processing activities.

(814) In this regard, the Commission considers that Alphabet's contractual arrangements towards third-party OSEs must not exceed what is necessary to ensure the anonymisation of the Search Dataset, as those measures, taken altogether, comprehensively mitigate the residual risks of re-identification. This measure further contributes to implement Article 6(11) of Regulation (EU) 2022/1925 in a manner that prevents Alphabet from imposing controls over unrelated processing operations, in particular over the third party's online search independent processing operations, thereby ensuring that there is no remaining imbalance of rights and obligations on third-party OSEs.

(815) Finally, Alphabet's claim that the Commission should be regarded as controller or joint controller for the processing and sharing of the Search Dataset under Article 6(11) of Regulation (EU) 2022/1925 is manifestly unfounded. The Commission's specification of compliance measures pursuant to implementing powers conferred by Article 8 of Regulation (EU) 2022/1925 constitutes an exercise of its regulatory function under Union law. In doing so, the Commission does not become a controller of the Search Dataset. Rather, it determines the legal conditions governing the legal obligation for the sharing and processing of ranking, click, query and view data for the purposes of ensuring effective compliance with Article 6(11) of Regulation (EU) 2022/1925.

4.4.4.2.2. Contractual obligations to ensure anonymisation from the third-party OSEs' perspective

(816) The Commission considers that, in order to mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk from the third-party OSEs' perspective, Alphabet must impose on them a set of contractual obligations which, together with and in combination with the technical measures set out in 4.4.4.1 and other contractual measures in section 4.4.4.2.3 and 4.4.4.2.4, anonymise end users' personal data.

(817) The proposed measures in this section address the residual risks of re-identification that could arise, intentionally or incidentally, out of the processing of the Search Dataset by third-party OSEs, within the scope of their activities, as sole eligible recipients of the Search Dataset under Article 6(11) of Regulation (EU) 2022/1925. The measures mitigating the risks of re-identification by 'any other person', namely unintended third parties which are not eligible recipients of the Search Dataset, are dealt with in section 4.4.4.2.3.1.

4.4.4.2.2.1. Measures

(818) The Commission considers that the following measures are required to specify how Alphabet must comply with its obligation under Article 6(11) of Regulation (EU) 2022/1925.

(819) *Effective control*: Alphabet must require the third-party OSE to maintain the Search Dataset within a processing environment under its effective control. Any processing of the Search Dataset by the third-party OSE's subcontractors must take place within that processing environment.

(820) *Segregated processing environment*: Alphabet must require the third-party OSE to process the Search Dataset exclusively within a logically and technically segregated processing environment so as to prevent linking between the Search Dataset and any

other auxiliary dataset accessible to the third-party OSE or its subcontractors. The segregated processing environment must ensure that:

(a) the Search Dataset cannot be queried jointly with auxiliary datasets;

(b) the Search Dataset cannot be copied, merged, synchronised, across the third party OSE's systems with auxiliary datasets;

(c) processing of the Search Dataset by the third-party OSE and its subcontractors is confined to that segregated environment.

(821) *Prohibitions against linking, re-identification and augmentation*: Alphabet must prohibit the third-party OSE from:

(a) Attempting to link the Search Dataset with auxiliary datasets at record level;

(b) Attempting to re-identify directly or indirectly end users, including by attempting to determine, learn or annotate which records relate to the same end users (i.e. "re-sessionisation"), in any way, such as semantic similarity, behavioural fingerprinting or other techniques, beyond any mini-sessions provided as part of the Search Dataset;

(c) Augmenting, enhancing, or processing the Search Dataset in a manner that reverses, weakens, or circumvents applied technical anonymisation measures, including attempts to infer or reconstruct truncated, generalised, or removed attributes.

(822) *Permitted purposes of use:* Alphabet must require the third-party OSE to use the Search Dataset solely for the permitted purpose of optimising or improving OSE services, including, for instance, search functionalities such as refining retrieval and ranking systems, SERP optimisation, web crawling and index building, and functionalities such as query analysis, spell-checking, auto-suggestion, auto-completion, and, where applicable, for the purpose of optimising and improving grounding systems and search capabilities for AI chatbots insofar as such AI chatbots rely on search retrieval functionalities.[1109]

(823) Alphabet must prohibit the third-party OSE from using the Search Dataset for other unrelated purposes.

(824) Alphabet may prohibit third-party OSEs from looking up and serving results directly to end users from the Search Dataset.

(825) *Testing safeguard:* where the permitted purpose under recital (822) involves the training or fine-tuning of machine learning models, including models supporting ranking, retrieval, or AI chatbot functionalities, Alphabet must require the third-party OSE to conduct pre-deployment evaluation of the model to ensure that it does not, under reasonably foreseeable inputs, reproduce data from the Search Dataset in a manner exposing end users to risks of re-identification.

(826) *Retention duration:* Alphabet must require the third-party OSE to retain the Search Dataset for a period of maximum 13 months.

(827) *Prohibition of onward sharing and disclosure:* Alphabet must prohibit the third-party OSE from disclosing, sharing, sublicensing, or otherwise making available any

[1109] For the avoidance of doubt, the permitted purpose only extends to optimising and improving grounding systems and search capabilities for AI chatbots. Training of the general-purpose LLM underlying the AI chatbot is excluded from the permitted purpose.

ranking, query, click, or view data forming part of the Search Dataset received pursuant to Article 6(11) of Regulation (EU) 2022/1925 to any third party[1110].

(828) *Governance and traceability:* Alphabet must require the third-party OSE to implement appropriate and proportionate governance and traceability measures enabling verification that the above prohibitions are complied with and that processing aligns with the permitted purpose. Such a measure must include the identification and documentation by the third-party OSE of:

(a) Automated systems and processes accessing the Search Dataset;

(b) Material processing operations involving the Search Dataset; and

(c) Models trained or fine-tuned using the Search Dataset that are subject to the testing safeguard provided for in recital (825), and results of this testing.

4.4.4.2.2.2. The Commission's assessment

(829) The Commission considers that to mitigate the residual likelihood of end user re-identification from the Search Dataset to an insignificant level of risk from the perspective of third-party OSEs recipients, Alphabet must impose a set of contractual obligations addressing the residual risk that remains despite the technical measures set out in section 4.4.4.1.

(830) The means reasonably likely to be used, taking into account the time, cost and manpower, to attempt re-identification of end users from the Search Dataset depend on the financial, computational, staff, and auxiliary data resources available[1111]. The Commission considers that, by the nature of their activity – providing OSE services – they are inherently capable actors, generally equipped with the technical expertise, analytical tools, and computational resources to process, link, or augment datasets in sophisticated ways. This technical capability means that, if not prohibited and restricted by a structural measure, a baseline residual risk of re-identification remains for all third-party OSEs. This baseline residual risk consists of the most realistic technical means through which some end users could likely still be re-identified, even after the application of technical measures by Alphabet.

(831) Alphabet claims that the proposed measures of the Preliminary Findings ignore that recipients are OSEs that have their own search data that they will inevitably combine with the Search Dataset (thereby creating re-identification risks that contractual measures cannot address).[1112] Contrary to that claim, the Commission considers that the proposed *prohibitions against re-identification, linking and augmentation*, *access control separation with auxiliary advertising and analytics datasets* as well as *permitted purposes of use* measures precisely tackled the residual risk of re-identification that could arise out of the linking of the Search Dataset with the third-party OSE's own proprietary search data or auxiliary advertising and analytics data. The Preliminary Findings therefore did not ignore but instead specifically addressed that residual risk through appropriate contractual measures designed to mitigate such risk.[1113]

1110 Third-party online search engines' subcontractors acting as processors or authorised sub-processors are not considered third parties in this context.

1111 For example, third-party online search engines receiving Search Data may have access to auxiliary data through advertising networks that might enable them to link Search Data to specific individuals. See also Joint Guidelines, Doc ID […], paragraph 185 and footnote 149.

1112 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 268-281.

1113 Preliminary Findings, paragraphs 493, 538-540, 544-556.

(832) The Commission nevertheless converges with the concern expressed by Alphabet[1114] that processing of the Search Dataset across long processing chains involving further dissemination of the Search Dataset to subcontractors is susceptible to amplify the risk of unauthorised access or disclosure. It may also amplify the risk of processing inconsistent with the contractual measures and restrictions imposed on the eligible third-party OSEs. The measure provided for in recital (795)(d) that third-party OSEs are responsible to pass-on contractual measures to their subcontractors acting as processors and sub-processors is meant to ensure continuity of those contractual measures ensuring anonymisation of end users' personal data as well as continued protection of the Search Dataset against unauthorised access or disclosure. However, the Commission considers that, alone, it is not equally effective to a structural and technical restriction against dissemination and linking of the Search Dataset.

(833) In light of the above, the Commission considers that the baseline risk identified in recital (830) justifies that Alphabet imposes a set of contractual restrictions and prohibitions on third-party OSEs to mitigate the residual risk of re-identification that remains despite the technical measures set out in section 4.4.4.1[1115] These restrictions and prohibitions should ensure that the Search Dataset is effectively protected against de-anonymisation.

(834) **First**, the Commission considers that the third-party OSE should be required to maintain the Search Dataset within a processing environment under its effective control and that any processing of the Search Dataset by the third-party OSE's subcontractors shall also take place within that processing environment.

(835) The Commission considers that this requirement is necessary to limit the dissemination of the Search Dataset and to reduce the number of entities, systems and processing environments to which the Search Dataset is exposed. While subcontractors may legitimately assist the third-party OSE in processing the Search Dataset on its behalf, the multiplication of processing chains and disclosure of the Search Dataset or part of it to distinct processing environments increases the risk of unauthorised access or processing inconsistent with the contractual measures required under Article 6(11) of Regulation (EU) 2022/1925 and specified under the present Decision to ensure anonymisation.

(836) The requirement of effective control does not imply that the Search Dataset must be processed on infrastructure owned or physically operated by the third-party OSE. In particular, the use of cloud infrastructure, managed hosting services, as well as subcontractors remains permissible, provided that the third-party OSE retains effective control over the processing environment in which the Search Dataset is processed and that the Search Dataset is not disclosed or replicated into separate processing environments outside that control.

(837) **Second**, the Commission considers that the third-party OSE should be required to process the Search Dataset exclusively within a logically and technically segregated processing environment to prevent linking between the Search Dataset and any other auxiliary dataset accessible to the third-party OSE or its subcontractors that could lead to a risk of re-identification. Such segregation does not require physical separation of infrastructure or dedicated computing clusters, but requires that the Search Dataset remain confined to a dedicated processing environment. It may be achieved through logical segregation mechanisms, including virtualisation, isolated workloads or other equivalent technical arrangements, provided that they effectively

1114 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 282 d).

1115 See also Expert Report On Anonymisation, section 6.2, Doc ID […].

ensure that the Search Dataset remains segregated from auxiliary datasets. In particular, access to the Search Dataset, data flows into and out of the processing environment, and processing operations performed within that environment must be governed in a manner that preserves the Search Dataset segregated from auxiliary datasets. In practice, the segregation will be supported by the *access control and access governance*, *data handling and other protection*, *logging, monitoring and accountability*, and *system security maintenance and vulnerability management* measures set out further in recitals (902), (903), (905) and (907). Those measures contribute to ensuring that access to the Search Dataset remains restricted to authorised personnel and systems, that the Search Dataset is not copied or transmitted outside the segregated processing environment, that compliance can be effectively verified and that the integrity of the segregated processing environment is maintained over time.

(838) The Commission considers that such segregation constitutes a further structural measure contributing to the set of measures aiming at effectively mitigating the residual risk that the Search Dataset could be linked with other datasets available to the third-party OSEs. In particular, the requirement that the Search Dataset cannot be queried jointly with auxiliary datasets, copied, merged, or synchronised across the third-party OSE's systems with auxiliary datasets ensures that processing of the Search Dataset remains confined to the segregated processing environment.

(839) However, the Commission notes that the *segregated processing environment* measure must not preclude third-party OSEs from subsequently using, deploying or further developing models that have been trained or fine-tuned on the Search Dataset, including through subsequent training or fine-tuning on other datasets, including the third-party's own search datasets, provided that the Search Dataset itself remains confined to the segregated processing environment and is not combined with such datasets.

(840) In that context, the Commission further concludes that a separate measure requiring access separation from advertising and analytics datasets is no longer necessary.[1116] The requirement that the Search Dataset be processed exclusively within a logically and technically segregated processing environment already ensures that the Search Dataset remains separated from any auxiliary dataset accessible to the third-party OSE or its subcontractors, whether advertising datasets or other proprietary datasets. This new broader segregated processing environment requirement therefore captures and extends the objective pursued by the previously proposed measure.

(841) In addition, the Commission finds that such a measure facilitates effective independent verification with the contractual measures set out in the present Decision. By requiring the Search Dataset to remain within a segregated processing environment under the effective control of the third-party OSE, the measures establish a clear identifiable audit perimeter for the audits to be performed in accordance with the independent verification mechanism set out in section 4.4.4.2.4. This enables the independent verifier to assess compliance within a defined set of systems, processing operations and controls, rather than having to examine a potentially larger number of systems and processing environments to which the Search Dataset may have been disseminated. The measure therefore increases the effectiveness and reliability of the verification process.

(842) **Third**, while the *effective control* and *segregated processing environment* measures establish structural safeguards restricting linking of the Search Dataset with auxiliary

[1116] Preliminary Findings, paragraphs 539 and 550.

dataset and preventing its dissemination to other processing environments, the Commission considers it necessary to impose prohibitions governing how the Search Dataset may be processed by the third-party OSE and its subcontractors. The *prohibitions against linking, re-identification and augmentation* are further measures necessary to address residual risks arising from processing activities conducted within the controlled and segregated environment.

(843) *In the first place,* the *prohibition against linking* reinforces the segregated processing environment requirement by prohibiting the third-party OSE and its subcontractors from combining the Search Dataset with auxiliary datasets at record level. Such a prohibition ensures that those entities remain subject to a clear conduct obligation not to engage in processing activities that could enable the singling out of individual records or the inference of additional attributes relating to them.

(844) *In the second place*, the *prohibition against re-identification* prevents the third-party OSE and its subcontractors from attempting, directly or indirectly, to identify end users in the Search Dataset. This includes attempts to determine, learn or annotate which records relate to the same end user ("re-sessionisation"), whether through semantic similarity, behavioural fingerprinting or other techniques, beyond any mini-sessions included in the Search Dataset. The Commission considers that such a prohibition is necessary to prevent downstream processing from undermining the effectiveness of the technical measures applied by Alphabet to reduce the risk of singling out and re-identification.

(845) *In the third place*, the *prohibition against augmentation* prevents the enrichment of the Search Dataset through the addition of attributes, identifiers or other information derived from auxiliary datasets or analytical techniques. The Commission considers that such a prohibition is necessary to prevent the Search Dataset from being supplemented with information that could facilitate singling out, linking or inference, including through attempts to infer, reconstruct or otherwise approximate metadata attributes that were truncated, generalised or removed as part of the technical measures applied by Alphabet. Such augmentation could increase the informational value of individual records and thereby undermine the effectiveness of those technical measures in reducing the residual risk of re-identification.

(846) **Fourth**, the Commission considers that the *permitted purposes of use* measure is complementary to the technical and contractual measures above, as they constrain the scope of processing in a manner that materially reduces the residual risks described in recital (837). Indeed, limiting the use of the Search Dataset to the optimisation or improvement of online search services reduces the likelihood that third-party OSEs would use it for other uses that could increase, even incidentally, re-identification risks. However, Alphabet must not unduly limit the legitimate purpose of use of the Search Dataset for improving and optimising online search engine services, as that would be contrary to the objective of Article 6(11) of Regulation (EU) 2022/1925 – which is to improve contestability and fairness in online search and considering that the third-party OSE acts as an independent controller (separate from Alphabet) when it processes personal data for that permitted purpose (see recital (808)).

(847) As set out in section 1.3, the Search Dataset provided under Article 6(11) of Regulation (EU) 2022/1925 can be used for many use cases which fall within the improvement or optimisation of OSE services. This is in line with recital 61 of that Regulation, which states that Search Data must be provided to undertakings providing OSEs so that they "*can optimise their services and contest the relevant*

core platform services". The recital does not put any limitation on this broadly framed purpose.

(848) In particular, contrary to Alphabet's narrow interpretation,[1117] the purpose of use of the Search Dataset must not be restricted to refining search algorithms alone. First, there is no such thing as a single search algorithm. OSEs rely on several different algorithms with different roles, which pass information to each other. For example, some main algorithms that Google Search relies on include the Glue algorithm, DeepRank algorithm, and Tangram algorithm.[1118] All such algorithms are in scope of the permitted purposes of use of the Search Data. Moreover, while search algorithms are indeed an important element of OSEs, and refining search algorithms is an important use case for the Search Data, OSEs rely on other elements too. Importantly, this includes:

(a) **Web crawling and index building.** As set out recital (18)(a), the cost involved in web crawling and index building is a major barrier to entry and expansion in online search, and the Search Dataset provided under Article 6(11) of Regulation (EU) 2022/1925 is valuable to inform third-party OSEs' crawling strategy and manage their crawling budgets.

(b) **Refining retrieval and ranking systems.** As set out in recital (18)(b), retrieval and ranking systems ensure that end users are presented with the most relevant results in relation to their query. Improving the ranking of such results requires analysis of user interaction data to understand which results received most user interest and engagement. Search Data provided under Article 6(11) of Regulation (EU) 2022/1925) is therefore crucial for the optimisation and improvement of retrieval and ranking systems

(c) **SERP optimisation systems:** As set out in recital (18)(c), search data is used to determine the SERP layout and the display of search results to the end users.[1119] Search Data provided under Article 6(11) of Regulation (EU) 2022/1925) is therefore needed to inform decisions on whether and when to present advanced search results modules, place specific URLs in dedicated parts of SERP, display of tabs, carousels, and rich results.

(d) **Query analysis and spell checking, auto-suggestion and auto-completion.** As set out in recital (18)(d), analysing queries to understand user intent and spell checking, auto-suggestion and auto-completion are important functionalities that shape user experience when using an OSE. Optimisation and improvement of these services is therefore an integral part of the permitted use of optimising online search services. The Search Dataset provided under Article 6(11) of Regulation (EU) 2022/1925 is valuable for the improvement of these functionalities, as it helps build understanding of user intent behind each query, informing which spell checks, auto-suggestions or auto-completion to display

(849) The above is not an exhaustive list. Search Data provided under Article 6(11) of Regulation (EU) 2022/1925 can aid third-party OSEs with a range of smaller sub-problems within the provision of OSE, such as optimising the modules on the SERP and when to surface (e.g., when and where to display advanced search results), detection of spam or other low-quality content, etc.

1117 Alphabet's response to the Revised Measures, Doc ID […], paragraphs 56-57.

1118 Alphabet presentation "Search data & algorithm development" of 2 March 2026, page 9.

1119 See, for example, Search Engine Results Page (SERP) available at What is a SERP? A Guide to Search Engine Results Pages | Definition from TechTarget.com, last accessed on 9 June 2026.

(850) Alphabet argues that there is a sharp division between (i) the developing of algorithms, which is an episodic task that happens at significant intervals, and (ii) producing results, which is a continuous task as a search engine operates. It argues that the Search Data may only be used for the first task.[1120] However, this is a false dichotomy. There is a spectrum of tasks that consist of frequent changes and continuous improvement, which sit between the infrequent updates to the whole algorithm and serving results. Examples are crawling, indexing, quality scoring of websites, updating spelling correction with new vocabulary, improving query understanding and expansion, and improving the triggering of advanced results modules. All such tasks rely on Search Data and the scale gap between Google Search and other OSEs contribute to the lack of contestability in online search.

(851) As set out in section 4.2, Article 6(11) of Regulation (EU) 2022/1925 does not have a "primary use" or "centre of gravity" test. This means that undertakings that offer an OSE in combination with other services (as Alphabet does) or as part of another service can be eligible beneficiaries of the Search Dataset. A notable example of this are undertakings providing AI chatbots. As explained in section 4.2, AI chatbots may need to retrieve fresh content to reply to certain user queries. They do so by passing a query to third-party or internal search infrastructure, and by passing the search results to the LLM. This process is typically called "grounding". Where the beneficiary uses the Search Dataset to improve or optimise search infrastructure or capabilities, including retrieval, ranking, indexing, query understanding or grounding capabilities, which are subsequently used to provide or support an OSE, this falls within the permitted purposes of use of Article 6(11) of Regulation (EU) 2022/1925. The Commission does not agree that the reference to grounding systems expands the permitted purposes of use beyond the optimisation or improvement of online search engine services.[1121] Grounding typically refers to the use of search retrieval infrastructure to obtain relevant and up-to-date information in response to a user query. Where the Search Dataset is used to improve or optimise retrieval, ranking, grounding or other search-related capabilities (e.g. query understanding) that form part of an OSE, such use remains within the permitted purpose of improving or optimising OSE services, irrespective of whether those capabilities are accessed through a traditional search interface or through an AI chatbot interface.

(852) For clarity, the specified measures do not impose on Alphabet an obligation to provide a syndication-like real-time grounding service.[1122] They rather specify that the Search Dataset can be used for improving OSE services, which are then used by AI chatbots for accessing information on the internet. This is in line with Alphabet's view that "*recipients are entitled to use the Search Dataset to optimise an online search engine that they make available to users, and they can use that online search engine also as a grounding tool for their AI chatbots*".[1123]

(853) At the same time, the Commission does not agree with Alphabet's view that the third-party OSEs cannot "*offer[] grounding services to third parties*" or to provide

---

1120 Alphabet presentation "Search data & algorithm development" of 2 March 2026, page 11.

1121 Alphabet's response to the Revised Measures, 15 June 2026, Doc ID […], paragraphs 76-83.

1122 Alphabet submits that "*to provide such grounding support, Google would have to implement a syndication-like service where chatbots would send queries to Google and Google would return search results in real time that the chatbots would use to generate their output*", which Alphabet disagrees with. However, Alphabet also states that "*nothing prevents recipients from using the search data disclosed under Art. 6911) to improve their search engine and then use that independently developed search engine for grounding an AI chatbots*." See Alphabet's submission of 14 April 2026, Doc ID […], paras 3 and 20. .

1123 Alphabet's response to the Revised Measures, 15 June 2026, Doc ID […], paragraph 81.

B2B OSE services which involve the Search Dataset.[1124] Once the Search Dataset is fed into third-party OSEs in line with the specified measures, it constitutes an inherent part of their OSE services, over which they can exercise their business freedom, including a freedom to use their OSEs to provide grounding services to other third parties. If Alphabet were permitted to determine the interfaces, distribution channels or business models through which competing undertakings may deploy OSE functionalities developed or improved using the Search Dataset, this would confer Alphabet the right for a perpetual control over such OSEs and subsequent transactions involving them. Such a right would run against third parties' business freedom, the free movement of services and could foreclose secondary markets.[1125] Such restrictions would also amount to an imbalance of rights and obligations on business users in contradiction with Article 8(8) of Regulation (EU) 2022/1925.

(854) In response to Alphabet's comment,[1126]regarding the statement in the footnote of the *permitted purposes of use* measure in recital (822) that "[t]raining of the general purpose LLM underlying the AI chatbot is excluded from the permitted purpose", the Commission clarifies that this exclusion only applies to the pre-training of the general purpose LLM underlying the AI chatbot. It does not extend to other AI systems to the extent that they are used for the purpose of optimising or improving OSE services as this would run against the objective pursued by Article 6(11) of Regulation (EU) 2022/1925 given that OSEs rely on input by AI systems other than the general purpose LLM underlying the AI chatbot, including query understanding, speech recognition, etc.

(855) Finally, the Commission considers that Alphabet may prohibit third-party OSEs from looking up and serving results to end users directly from the Search Dataset as Article 6(11) is not intended to establish a search syndication regime under which third-party OSEs merely reproduce search results generated by Alphabet's Google Search OSE.

(856) **Fifth**, the Commission considers that a testing safeguard is appropriate to address the residual risk identified by the EDPB that machine learning models trained or fine-tuned on the Search Dataset could, in exceptional circumstances, reproduce information derived from the Search Dataset through model outputs. [1127] The Commission notes that the technical and organisational measures imposed on the Search Dataset are designed to prevent direct and indirect identification of end users and substantially reduce the likelihood that personal data relating to individual end users are present in a form capable of being learned and reproduced by downstream models.

(857) Therefore, given the extensive technical measures applied to the Search Dataset (see section 4.4.4.1.1), the Commission considers that the risk that a downstream model could memorise and subsequently reproduce a specific data pattern derived from the Search Dataset in a manner that could contribute to the re-identification of an end user or the attribution of information to that end user constitute a remote residual risk. The Commission further notes that memorisation alone does not give rise to such risks. The relevant concern is limited to the exceptional circumstance where

1124 Alphabet's response to the Revised Measures,15 June 2026, Doc ID […]paragraphs 78-83.
1125 See the doctrine of exhaustion in IP law.
1126 Alphabet's response to the Revised measures, 15 June 2026, Doc ID […], paragraph 110.
1127 EDPB comments on the proposed measures of 5 May 2026, Doc ID […], paragraph 13.

reproduced information is sufficiently distinctive and attributable to an identifiable individual so that it could enable direct or indirect re-identification.

(858) In consideration of that remote and, in any case very limited, residual risk, the Commission considers that a targeted pre-deployment evaluation constitutes an appropriate and proportionate additional safeguard to further mitigate that risk. The measure does not require continuous monitoring of downstream processing activities, nor does it impose extensive testing obligations beyond those necessary to assess reasonably foreseeable model behaviour before deployment. Rather, it seeks to provide assurance that downstream models do not operationalise the Search Dataset in a manner that could expose end users to risks of re-identification through the unintended reproduction of information derived from that dataset.

(859) Alphabet submits that the testing safeguard should be expanded to require periodic testing and that the reference to "*models supporting AI chatbot functionalities*" is inconsistent with the *permitted purposes of use* measure because such models allegedly fall outside the permitted uses of the Search Dataset.[1128] The Commission disagrees. The *testing safeguard* does not define or expand the permitted purposes of use of the Search Dataset. Rather, it applies where a model is trained or fine-tuned using the Search Dataset in accordance with the *permitted purposes of use* measure and serves solely to address the specific residual risk that information derived from the Search Dataset could be reproduced through model outputs in a manner exposing end users to risks of re-identification. Accordingly, the reference to "*models supporting AI chatbot functionalities*" cannot be understood as permitting the use of the Search Dataset for purposes that fall outside the *permitted purposes of use* specified in this Decision. In addition, the Commission does not consider periodic or ongoing testing necessary or appropriate for the purposes of the testing safeguard. Periodic testing would transform the targeted and proportionate *testing safeguard* measure into a continuing obligation extending throughout the lifecycle of the model and potentially beyond the period during which access to the Search Dataset is provided under contractual arrangements with Alphabet. To the extent that a third-party OSE subsequently operates, modifies or further develops such models, including in circumstances involving the processing of personal data (for ex with its own proprietary search data), it remains subject to its own obligations under Regulation (EU) 2016/679. The Commission therefore does not consider it necessary to impose an additional recurring testing obligation in the present Decision.

(860) **Sixth**, the Commission considers that a contractual measure limiting the *retention duration* of the Search Dataset is necessary. Limiting retention duration generally reduces the volume of data held at any given time, thereby proportionally reducing exposure to security risks and potential misuse, irrespective of technological evolution. At the same time, a minimum period of 13 months appears necessary to ensure that third-party OSEs can train and optimise their algorithms in a manner that captures seasonal and annual trends in search behaviour as indicated by some third parties.[1129] In this context, the Commission considers that retaining the Search Dataset for a period of 13 months allows third-party OSEs to observe full yearly cycles, detect trends, and optimise services, while limiting the risk of long-term retention that could increase re-identification risks.[1130]

1128 Alphabet's response to the Revised Measures, 15 June 2026, Doc ID […], paragraphs 114-116.

1129 [Market participants]'s reply to RFI of 18 November 2025, Doc ID […], question 12, page 11; [market participant]'s reply to RFI of 18 November 2025, Doc ID […]1, question 12, page 9.

1130 Secure erasure mechanisms are addressed in section 4.4.4.2.3.1.

(861) **Seventh**, the Commission considers that the *Prohibition on onward sharing and disclosure* of the Search Dataset to any third party is necessary in order to ensure that only eligible recipients, and its subcontractors acting on behalf of the third-party OSE under equivalent contractual obligations, are granted access to the Search Dataset. Access to the Search Dataset is limited to eligible third-party OSEs that comply with the contractual measures imposed by Alphabet, including the prohibitions aimed at mitigating the residual risks of singling out, linking and inference. Allowing onward sharing beyond that controlled circle would enable entities that have not been assessed against those eligibility conditions, and that are not subject to equivalent obligations or to the independent verification mechanism, to obtain access to the Search Dataset, thereby increasing the likelihood that the data could be processed in a manner that would undermine the anonymisation framework.

(862) **Eighth**, the Commission considers that appropriate and proportionate *governance and traceability* requirements are necessary to support the monitoring, auditability and enforceability of the contractual measures.[1131] Appropriate documentation enables independent auditors and, where relevant, competent authorities to assess whether the Search Dataset has been processed in accordance with the applicable restrictions and to detect potential instances of non-compliance.

(863) In particular, the Commission considers that governance and traceability obligations must ensure that the third-party OSE can identify the systems, processing operations and models that access or use the Search Dataset while it remains within the segregated processing environment. In addition, the Commission considers it necessary to identify and document the models trained or fine-tuned using the Search Dataset until they have successfully undergone the testing required in recital (825) and the results of that testing have been documented. At that stage, the Commission considers that the governance and traceability obligations relating to the Search Dataset are no longer necessary as the likelihood of re-identification of end users has been mitigated to an insignificant level. The Commission indeed considers that the introduction of the *testing safeguard* in the Decision makes it possible to define with appropriate legal certainty the material and temporal scope of the *governance and traceability* obligations measure.[1132] As explained in recital (853), once the Search Dataset is fed into third-party OSEs in line with the specified measures, including the *testing safeguard* measure verifying that models trained or fine-tuned using the Search Dataset do not expose end users to risks of re-identification, it constitutes an inherent part of their OSE services, over which they can exercise their business freedom.

(864) Contrary to Alphabet's position, the Commission does not consider it necessary or proportionate in light of the *testing safeguard* measure described above to require exhaustive or perpetual documentation of all downstream processing activities, datasets or models irrespective of the degree to which they are derived from the Search Dataset.[1133] Such an approach would require the continued and indefinite traceability of datasets and models, including after a model trained or fine-tuned using the Search Dataset has successfully undergone the testing required in recital (825) and the results of that testing have been documented, while providing no additional value to the verification of compliance with the contractual measures.

1131 Joint Guidelines, Doc ID […], paragraph 181 and 189.

1132 This also addresses Alphabet's claim according to which the proposed Governance and traceability measure in the Preliminary Findings (paragraph 543) was vague and could create contractual ambiguity, see Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 573-574.

1133 Alphabet's response to the Revised Measures, dated 15 June 2026, Doc ID […], paragraphs 111-113.

Requiring documentation beyond what is necessary for such verification that contractual measures have been complied with would exceed what is required to ensure effective accountability and would impose disproportionate technical and operational burdens on third-party OSEs. Such an approach would also extend the audit scope beyond what is necessary to verify compliance with the contractual measures whereas the risks of end users' re-identification are insignificant. The Commission therefore considers that governance and traceability obligations must remain limited to what is necessary to enable meaningful auditability and verification of compliance with the contractual measures, thereby ensuring an appropriate balance between enforceability and proportionality.

(865) The Expert Report on Anonymisation proposes an additional contractual measure of prohibition against record-level employee access to mitigate the specific risk of indiscreet employees misusing the Search Dataset.[1134] However, the Commission considers that, while such a measure may be appropriate, the risk of employee misuse is already mitigated by other contractual measures, and imposing such a restriction as a general requirement could create constraints that may not ensure access on FRAND terms for certain potential third-party OSE beneficiaries.

(866) Some beneficiaries confirmed that, in practice, access to record-level data by specialised teams and personnel is frequent and necessary for legitimate operational purposes, such as debugging, quality evaluation or security-related reasons and that requiring prior authorisation for every access to a record could create disproportionate operational constraints that would affect access on FRAND terms for smaller third-party OSEs.[1135] In that context, the Commission considers that the residual risk of employee misuse of the Search Dataset is already adequately mitigated by the specified contractual measures. In particular, the *prohibitions against linking, re-identification, and augmentation* (recital (819)), the *permitted purposes of use* (recital (822)), the *access control and governance* (recital (902)), *logging and monitoring* (recital (905)), *data breach reporting* measures (recital (908)), as well as the independent verification mechanism (section 4.4.4.2.4) together ensure that only authorised personnel may access the Search Dataset at record-level for the permitted uses, on a need-to-know basis, and that any misuse would be detected and addressed. Given this comprehensive framework, the Commission considers that it will be for the independent auditor, acting in accordance with the verification mechanism set out in section 4.4.4.2.4 to assess whether the technical, organisational and human controls implemented by a given third-party OSE provide reasonable assurance of compliance with those obligations, taking into account its specific risk profile, size, and organisational structure.

4.4.4.2.2.3. The Commission's assessment of Alphabet's claim that contractual measures are not permissible means to ensure anonymisation

(867) In essence, Alphabet submits that contractual measures cannot constitute valid legal means capable to effectively mitigate the risks of end users' re-identification.[1136]

(868) **First**, the Commission disagrees with Alphabet's contention that only technical measures may be taken into account when assessing whether end users' personal data

---

1134 Expert Report On Anonymisation, Doc ID […], section 6.2.6.

1135 [Market participants]'s reply to RFI of 12 February 2026, Doc ID […], questions 5 and 6, ppage 5-6; [market participant]'s reply to RFI of 12 February 2026, Doc ID […], questions 5 and 6, page 4-5.

1136 See recital (588) of the present Decision and Alphabet's response to the Preliminary Findings, chapter 2, section V, Doc ID [...].

are anonymised and that contractual measures cannot constitute valid legal means capable of effectively contributing to the anonymisation of end users' Search Data.

(869) *In the first place*, Article 6(11) of Regulation (EU) 2022/1925 read in light of recital 61 does not mandate that personal data of end users be anonymised before sharing with third-party OSEs on the basis of technical measures *only*, thereby excluding that contractual measures could effectively contribute to mitigating the likelihood of end users' re-identification to an insignificant level. Instead, it provides that "[w]*hen providing access to its search data, a gatekeeper should ensure the protection of the personal data of the end users, including against possible re-identification risks, by appropriate means, such as anonymisation of such personal data, without substantially degrading the quality and usefulness of the data*." (emphasis added). While the Commission aligns with the expert legal opinion of 25 March 2026 that in the present case technical measures are indispensable and that measures other than technical ones are not sufficient on their own to ensure anonymisation,[1137] the Commission considers that the reference to "*appropriate means*" does not prescribe a single category of means (i.e. technical means). Instead, the Commission considers that the assessment of the anonymisation of end users' personal data must be carried out taking into account all appropriate means, including not only the indispensable technical means but also other appropriate means (i.e. organisational, administrative and contractual) under which such access is granted, insofar as those means, taken together, effectively mitigate the risk of re-identification while preserving the quality and usefulness of the data.[1138]

(870) *In the second place*, as explained in recital (555), the Commission is of the view that the assessment of whether identification is reasonably likely must take into account the legally binding conditions under which access to the ranking, query, click and view data is granted pursuant to an implementing act of the Commission specifying the technical and contractual measures to be applied by the gatekeeper, insofar as those measures produce a durable and verifiable effect.[1139] As a result, by specifying those legally binding conditions in an implementing act under Article 8(2) of Regulation (EU) 2022/1925, including relevant contractual prohibitions or restrictions under which third-party OSEs must be subject to protect end users against re-identification, the present Decision imposing contractual measures constitute legal means capable to effectively mitigate the residual risks of re-identification to an insignificant level and thereby to achieve anonymisation from the perspective of third-party OSEs.

(871) *In the third place*, the Commission further disagrees with Alphabet's claim that the specified contractual measures would have no effect on third-party OSEs because the specification measures formally bind Alphabet only. While the present Decision is addressed to Alphabet, the contractual measures imposed on third-party OSEs will derive their practical effect from Alphabet's obligation to require, monitor and enforce compliance with those contractual measures. Third-party OSEs applying for eligibility to the Search Dataset must agree to those conditions, and failure to comply may result in suspension or termination of access to the Search Dataset (see sections 4.6.7.2, 4.6.7.3 and 4.6.7.4). Accordingly, the contractual measures are not detached from the regulatory framework established by the present Decision but form an

---

1137 See Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], page 21 referring to the Commission's own position in the Joint Guidelines, Doc ID […], paragraph 181 and 189.

1138 Recital 61 of Regulation (EU) 2022/1925 and Joint Guidelines, Doc ID […], paragraph 181.

1139 Joint Guidelines, Doc ID […], paragraphs 181 and 187 to 189.

integral part of the effective compliance mechanism through which Article 6(11) of Regulation (EU) 2022/1925 is implemented.

(872) *In the fourth place*, the Commission considers that such an approach is consistent with the settled case law of the Court of justice in *Breyer* judgment according to which data subjects are not identifiable with means reasonably likely to be used where identification of the data subjects is "*prohibited by law or impossible in practice*" (emphasis added), so that the risk of identification appears in reality to be insignificant.[1140] Alphabet's insistence that anonymisation requires to render identification practically impossible[1141] overlooks the fact that the Court expressly recognises that legal restrictions on identification are relevant, independently of whether identification is impossible in practice, when assessing whether means of identification are reasonably likely to be used in the specific circumstances of a given case.

(873) In line with further relevant case law of the Court of justice, the Commission considers that, under the specific circumstances of the case and taking into account the legally binding conditions set out in the present Decision, third-party OSEs, as recipients of the Search Dataset, are not in a position to lift the technical measures implemented by Alphabet during any processing of the Search Dataset carried out under their control and that the contractual measures imposed on them are as such as to prevent those third-party OSEs from attributing record level Search Data forming part of the Search Dataset to any end user, including by a wide range of means,[1142] in such a way that, for those third-party OSEs, the end users are no longer identifiable.[1143]

(874) **Second**, the Commission considers that the legally binding conditions set out in the present Decision, including mandating contractual measures to ensure anonymisation of end users' personal data from the perspective of the third-party OSE recipients or of any other person, ensures that end users' personal data are not processed by the third-party OSE and therefore fundamental rights to private life and personal data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights are protected. Alphabet's claim that they would violate end users' fundamental rights to informational self-determination of end users is unfounded.

(875) *In the first place*, the purpose of the technical and contractual measures specified by the Commission is precisely to ensure anonymisation of end users' personal data when the Search Dataset is shared with eligible third-party OSEs, in accordance with the legal obligation established in Article 6(11) of Regulation (EU) 2022/1925. Anonymisation of the end users' personal data in the Search Dataset ensures that that information cannot be linked by the third-party OSE to end users and therefore their rights guaranteed by Articles 7 and 8 of the Charter are protected while allowing the contestability objective pursued by Article 6(11) of Regulation (EU) 2022/1925 to be achieved.

(876) *In the second place,* the fact that end users' data would become personal data again in the case of breach of the contractual measures does not leave the classification of

---

1140 Judgment of the Court of Justice of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016-779, paragraphs 45-46.

1141 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 135-147.

1142 The contractual measures comprehensively address the risks of linking, of re-identification via singling out (i.e., re-sessionisation) and inference that could arise from downstream processing that could undermine the effectiveness of the technical measures applied by Alphabet.

1143 Judgment of the Court of Justice of 4 September 2025, *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025-645, paragraphs 86 and 87.

Search Data in an indeterminate state, contrary to Alphabet's claim. On the contrary, the legal classification of personal data depends on whether measures effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.[1144] In the case at hand, where the technical and contractual measures imposed by the present Decision are complied with, end users' Search Data are anonymised from the perspective of the third-party OSE recipient. By contrast, where a third-party OSE breaches those contractual measures, the Commission considers that risks of re-identification of end users must be considered as increased beyond an insignificant level, rendering end users' Search Data personal data again from the perspective of that third-party OSE.

(877) *In the third place*, Alphabet's claim incorrectly suggests that end users would be left without any legal protection vis-à-vis third-party OSEs recipients of the Search Dataset. That is not the case. As indicated in recital (1345), Alphabet must maintain on its website a page listing the third-party OSEs that have received access to the Search Dataset and must display on this page a notice in respect of each eligible third-party OSE publicising that Level 1 and Level 2 assurance has been obtained as well as a notice publicising the fact of any termination and expedited termination decisions. These notices provide end users, other individuals and civil society organisations with a basis to exercise their right to lodge a complaint with competent supervisory authorities under regulation (EU) 2016/679 to investigate the circumstances which led to the termination or expedited terminations decisions. In cases where those circumstances are the result of a processing of end users' personal data in violation of the contractual measures imposed by Alphabet to ensure anonymisation, that processing of personal data could fall under the scope of Regulation (EU) 2016/679 and, in the absence of a valid lawful ground under Articles 6 and 9 of that Regulation, may give rise to responsibility and liability of the third-party OSE. It follows that the measures do not deprive end users or other individuals of their right to lodge complaints with competent supervisory authorities or to seek judicial remedies and compensation under Articles 77, 79 and 82 of Regulation (EU) 2016/679 in the event that a third-party OSE unlawfully processes personal data, including through breaches of the contractual measures designed to ensure anonymisation.

(878) *In the fourth place*, the Search Dataset remains subject to the protections afforded by Chapter V of Regulation (EU) 2016/679 before the sharing takes place to the extent it also contains personal data of other individuals than end users while the *effective control*, *segregated processing environment* and *prohibition on onward sharing and disclosure* measures ensure that the shared Search Dataset remains within the third-party OSE's environment and cannot be subsequently transmitted or transferred to any third party or third country. Alphabet's suggestion that the Search Dataset would be exposed to loopholes of protection in that regard is therefore equally unfounded.[1145]

(879) **Third**, Alphabet's argument according to which recipients will inevitably combine the Search Dataset with their own search data or other auxiliary datasets and that contractual restrictions cannot effectively prevent such conduct cannot be accepted.

1144 Judgment of the Court of Justice of 4 September 2025, *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025-645, paragraphs 84, 86 and 87.

1145 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 282-283.

(880) Taken to its logical conclusion, that claim would deprive Article 6(11) of Regulation (EU) 2022/1925 of its practical effect. As Alphabet itself notes, a significant proportion of users of competing third-party OSEs also use Google Search.[1146] However, if the existence of overlapping user base were sufficient to render the combination of datasets inevitable and incapable of being prevented through the contractual measures specified by the present Decision, Article 6(11) of Regulation (EU) 2022/1925 could never operate in relation to its intended beneficiaries. If accepted, that reasoning would imply that any disclosure of search data under Article 6(11) of Regulation (EU) 2022/1925 necessarily creates an unacceptable re-identification risk, because every eligible third-party OSE invariably have at its disposal other information that could theoretically be combined and lead to an increase of the re-identification risks. The Commission cannot accept an interpretation under which the very market circumstances that justified the legislator's decision to introduce the obligation to share search data under Article 6(11) of Regulation (EU) 2022/1925 simultaneously render compliance with that provision impossible.

(881) Instead, the Commission considers that the contractual measures specified in the present Decision are effective in ensuring that third-party OSEs cannot combine the Search Dataset with auxiliary datasets. As explained in recitals (834) to (845), the *effective control*, *segregated processing environment* and *prohibitions against linking, re-identification and augmentation measures*, considered together, effectively prevent the risk that the Search Dataset be combined with search data of the third-party OSEs or other auxiliary data at their disposal (e.g. advertising dataset or other).

(882) **Fourth**, the Commission disagrees with Alphabet that reliance on contractual measures is legally inappropriate and ineffective because the harm for users from a data breach involving the Search Dataset would be serious and irreparable.

(883) *In the first place,* the Commission considers that Search Data is subject to extensive technical measures that mitigate risks of re-identification to a residual level. Consequently, a data breach involving the Search Dataset would expose significantly less information and create materially lower risks for affected individuals than a breach affecting Alphabet's own search records, which associate historical search logs with individual end user. Alphabet therefore overstates the seriousness of the residual risk associated with the Search Dataset in the case of unlawful access by an unintended third party.

(884) *In the second place,* any harm resulting from a breach cannot be characterised as irreparable in a legal sense. As explained above, end users retain the rights and remedies available under Regulation (EU) 2016/679, including the right to seek judicial remedies and compensation for material or non-material damage suffered as a result of the unlawful processing of their personal data in case the data are de-anonymised. The existence of such remedies confirms that the potential harm, the risks of which are mitigated to an insignificant level through technical and contractual measure, is not beyond legal redress. Accordingly, the mere possibility of a breach does not justify disregarding contractual measures as an appropriate component of the overall framework designed to protect end users against risks of re-

[1146] Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 127: "(…) Overall, based on Similarweb data, around 95% of ChatGPT users, 62% of Bing users, 89% of DuckDuckGo users, and 69% of Qwant users also use Google."

identification while ensuring the effectiveness of Article 6(11) of Regulation (EU) 2022/1925.

(885) **Fifth**, the Commission maintains its assessment that the commercial incentives of third-party OSEs are aligned with maintaining continued access to the Search Dataset rather than engaging in conduct that would jeopardise such access and disagrees with Alphabet that the contracts do not foresee consequences that are capable of dissuading breaches.

(886) Access to the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925 constitutes a key mechanism enabling third-party OSEs to improve the quality and competitiveness of their services vis-à-vis Google Search. Any attempt to re-identify end users or otherwise circumvent the applicable technical and contractual measures would expose the third-party OSE to the risk of suspension or termination of access to the Search Dataset as well as regulatory consequences (see below in sections 4.6.7.2, 4.6.7.3 and 4.6.7.4.). The loss of access to the Search Dataset would significantly undermine the ability of third-party OSEs to improve relevance, ranking quality and innovation, thereby weakening their capacity to effectively compete with Google Search.

(887) In addition, as explained in sections 4.4.4.2.4.1 and 4.6.6 both initial access to the Search Dataset and the maintenance of such access are conditional upon the provision of an independent assurance report concluding, with a reasonable level of assurance, that the third-party OSE meets the Commission-defined assurance objectives, as well as upon the payment of a fee (see section 4.5). Although these conditions are designed to ensure access to the Search Dataset on FRAND terms, they nonetheless require the third-party OSE to make significant human and financial investments, which would be rendered futile in the event of non-compliance and subsequent suspension or termination of access.

(888) Moreover, third-party OSEs have independent commercial incentives to maintain end users' trust in their own search services. Engaging in conduct aimed at re-identifying Alphabet's end users could also undermine the credibility of the third-party OSE's own services and damage its reputation among its own end users and business partners.

(889) By contrast, the potential commercial benefit that a third-party OSE could derive from attempting to re-identify individual users from the Search Dataset appears limited. In particular, re-identification would not materially contribute to the primary purpose for which the Search Dataset is made available, namely improving search relevance, ranking quality and innovation. The suspension and termination of access to the Search Dataset exposes third-party OSEs to regulatory consequences that Alphabet cannot discard. Regulation (EU) 2016/679 establishes a comprehensive enforcement framework under which infringements may give rise to significant financial and regulatory consequences. Accordingly, a third-party OSE considering conduct aimed at re-identification of Alphabet's end users would need to take into account not only the risk of losing access to the Search Dataset and potential significant investment incurred to get the data, but also the risk of administrative fines under Regulation (EU) 2016/679 which are specifically designed to be effective, proportionate and dissuasive. [1147]

(890) In this context, the potential gains from such conduct appear clearly outweighed by the substantial risks associated with breaching the applicable safeguards, including

[1147] Article 83 of Regulation (EU) 2016/679.

the possible suspension or termination of access to the Search Dataset, the resulting negative impact on the ability of the third-party OSE to develop and improve its services and the regulatory consequences and sanctions under Regulation (EU) 2016/679.

(891) The Commission therefore considers that the incentive structure created by Article 6(11) of Regulation (EU) 2022/1925 together with an implementing act under Article 8(2) of that Regulation specifying the legally binding conditions under which Alphabet must grant, suspend and terminate access to the Search Dataset pursuant to that provision further reduces the likelihood that third-party OSEs could re-identify or even attempt to re-identify end users to an insignificant level.

(892) **Sixth**, Alphabet's criticism that the Commission places an "unwarranted degree of trust" in third-party OSEs' incentives to abide by the contract[1148] is unfounded. Alphabet's criticism is based on the premise that the Commission's assessment of anonymisation would rely primarily on the assumption that third-party OSEs lack incentives to attempt re-identification. That premise is incorrect.

(893) The Commission's assessment does not conclude that end users' personal data are anonymised because third-party OSEs are unlikely to engage in re-identification. On the contrary, the assessment is primarily based on the objective characteristics of the dataset following implementation of the technical measures for the alteration of the Search Data and the cumulative effects of the legally binding conditions imposed by the present Decision consisting in a set of contractual measures, an independent verification mechanism, and a thorough process governing access to and use of the Search Dataset. In this context, the existence of an independent verification mechanism is difficult to reconcile with an assessment premised on an unwarranted degree of trust in third-party OSEs' compliance.

(894) The Commission's assessment regarding lack of incentives in the Preliminary Findings as reiterated above in recitals (885) to (891) responds to Alphabet's own argument (as also advanced in the expert opinions it commissioned[1149]), according to which third-party OSEs would have a high commercial incentive to re-identify users. The Commission explained why it does not share that assessment. Those recitals do not establish anonymisation based on an incentive analysis alone, but rebut Alphabet's own argument that third-party OSEs should be assumed to have a strong motivation to circumvent the applicable technical and contractual measures ensuring anonymisation.

(895) Seventh, the Commission does not agree that the national administrative decisions and judgments relied upon by Alphabet support its conclusions that the Search Dataset remains personal data because at least some individuals could still be identified by reasonably likely means and because contractual measures cannot remedy that circumstance.[1150] This is because the circumstances of the present data sharing are fundamentally different, which makes the analysis in the administrative decisions and judgments relied upon by Alphabet non transposable.

1148 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 288 – 289.

1149 Alphabet's Expert Opinion: Interplay between the Anonymisation Requirement under Article 6(11) of the DMA and the GDPR of 25 March 2026, Doc ID […], page 18. See also initial Alphabet's Expert Opinion: the Anonymisation Requirement under Article 6(11) of the DMA in the context of the GDPR of 18 November 2024, Doc ID […], paragraph 38.

1150 Alphabet's Observations on the Hiding Nemo Report, dated 17 June 2026, Doc ID […], paragraphs 80-88.

(896) *In the first place*, the Commission observes that the national decisions from data protection supervisory authorities and judgments relied upon by Alphabet concern assessment of anonymisation of datasets or information that either contained persistent individual-level identifiers enabling the longitudinal monitoring of individuals or the reconstruction of detailed user profiles or were made publicly available online. It follows that the factual circumstances in those cases are not comparable to the Search Data sharing framework contemplated by Article 6(11) of Regulation (EU) 2022/1925 and the legally binding conditions provided for in the present Decision:

(a) The *OC v European Commission* judgment of the Court of justice relied upon by Alphabet in support of its position concerned disclosure of information to the public via publication online,[1151] whereas the Search Dataset is made available only to eligible third-party OSEs and is subject to technical and contractual measures specifically designed to prevent the re-identification of end users;

(b) The *IQVIA* decision of the French data protection supervisory authority ('CNIL') does not support Alphabet's position. In that decision, the CNIL assessed whether the data remained personal data from the perspective of IQVIA itself, which controlled the overall processing operation and had defined the pseudonymisation process. Relying on the judgment of the Court of justice in *SRB v EDPS*,[1152] the CNIL expressly distinguished that situation from the position of a recipient of pseudonymised data whose ability to identify individuals must be assessed in light of the circumstances applicable to that recipient.[1153] The CNIL further relied on the fact that the datasets at issue enabled longitudinal monitoring of individual patients through a unique identifier and the reconstruction of detailed patient histories.[1154] Those circumstances are materially different from the Search Data sharing framework established by the present Decision, which does not provide third-party OSE recipients of the Search Dataset with any persistent end-user identifier enabling comparable longitudinal monitoring via the reproduction of end-user sessions (i.e. "re-sessionisation");

(c) Likewise, CNIL's decision of 15 June 2023[1155] and the Austrian data protection supervisory authority decision ('DSB') in *Google Analytics*[1156] concerned persistent pseudonymous online identifiers associated with individual users across multiple interactions over time. The CNIL and DSB's assessments were therefore based on processing operations that depended on maintaining a link to particular individuals through such persistent pseudonymous identifiers. By contrast, the Search Dataset does not provide third-party OSE recipients with

---

1151 Judgment of the Court of Justice of 7 March 2024, *OC v Commission*, C-497/22 P, ECLI:EU:C:2024:215, paragraph 22.

1152 Judgment of the Court of Justice of 4 September 2025, *EDPS v. SRB*, C-413/23 P, ECLI:EU:C:2025-645.

1153 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte SAN-2026-008 of 26 May 2026, *IQVIA OPERATIONS France*, paragraphs 88-90.

1154 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte SAN-2026-008 of 26 May 2026, *IQVIA OPERATIONS France*, paragraphs 91-94.

1155 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte SAN-2023-009 of 15 June 2023.

1156 Austrian Data Protection Authority (Datenschutz behörde or "DSB"), Decision of 22 December 2021, Case No. DSB-D155.027.

any persistent identifier enabling the continuous recognition or tracking of particular end users;

(d) The Irish data protection supervisory authority's decision ('IE DPC') concerning *WhatsApp* concerned data derived from telephone numbers, which are direct identifiers, and assessed whether such data remained attributable to identifiable individuals from the perspective of WhatsApp itself taking into account its system environment. The assessment relied in particular on WhatsApp's ability to relate the transformed data back to the underlying telephone numbers and combine the data derived from the telephone numbers with other information available within its own systems.[1157] The decision therefore concerned pseudonymised data that remained personal data from WhatsApp's perspective because WhatsApp itself retained the means to attribute the data to identified individuals. By contrast, eligible third-party OSE recipients do not have access to Alphabet's systems, are not provided with any comparable identifier and receive the Search Dataset only under the Search Data sharing framework established by the present Decision.

(897) *In the second place*, none of the decisions or judgments relied upon by Alphabet concerned a data sharing framework subject to legally binding conditions comparable to those established by Article 6(11) of Regulation (EU) 2022/1925 and the specification measures provided for in the present Decision. In particular, none involved a regulatory regime under which access to the data is conditioned upon a combination of technical and contractual measures that are imposed by a public authority and that are legally binding on the recipient of that Decision (i.e. Alphabet) so that neither the sender (i.e. Alphabet) nor the recipient (i.e. third-party OSEs) of the Search Dataset are in a position to modify or lift those technical and contractual measures ensuring end users' anonymisation.

(898) Considering all the above, the Commission concludes that the technical measures, in combination with the set of contractual measures and the independent verification mechanism established in section 4.4.4.2.4 mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk from the perspective of third-party OSEs in such a way that, for those third-party OSEs, the end users are no longer identifiable.

4.4.4.2.3. Integrity and confidentiality of the Search Dataset to ensure anonymisation against any other third person

(899) The Commission considers that, to mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk vis-à-vis any other third person, namely unintended third parties that are not eligible recipients of the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925, Alphabet must require third-party OSEs to comply with a set of contractual obligations which constitute the essential safeguards necessary to ensure the integrity and confidentiality of the Search Dataset.

4.4.4.2.3.1. Measures

(900) Alphabet must require the third-party OSE to implement and maintain the following organisational, administrative and contractual measures, which constitute essential safeguards necessary to protect the integrity and confidentiality of the Search Dataset, including protection against unauthorised or unlawful access, disclosure,

[1157] Irish Data Protection Commissioner Decision of 20 August 2021, WhatsApp, IN-18-12-2, paragraphs 107-110.

alteration or loss, taking into account the risks arising from its processing and recognised industry standards for the protection of sensitive datasets:

(901) *Technical protection of the Search Dataset*: Alphabet must require the third-party OSE to ensure that the Search Dataset is encrypted when stored in any system or environment under the third-party OSE's control and is encrypted during transmission between systems and environments, using state-of-the-art encryption appropriate for the sensitivity of the Search Dataset and the risks it is intended to mitigate, including unauthorised access resulting from physical loss or theft of storage media, together with appropriate cryptographic key management measures, including secure storage, access restriction, rotation and revocation of encryption keys.

(902) *Access control and access governance measures*: Alphabet must require the third-party OSE to:

(a) restrict access to the Search Dataset to personnel authorised by the third-party OSE, as well as to systems, strictly necessary for the permitted purpose of use (see recital (822))

(b) to assign access rights to such authorised personnel in accordance with the principles of least privilege[1158] and need-to-know[1159] and to periodically review and revoke access rights to the Search Dataset where such access is no longer necessary;

(c) to subject authorised personnel with access to the Search Dataset to phishing-resistant multi-factor authentication;

(d) ensure that authorised personnel with access to the Search Dataset are subject to enforceable confidentiality obligations and receive yearly training regarding access restrictions, secure handling and authorised and prohibited uses of the Search Dataset, as well as on applicable governance and traceability documentation obligations.

(903) *Data handling and other protection measures:* Alphabet must require the third-party OSE to prohibit the copying, downloading or local storage of any data from the Search Dataset on any other device, including authorised personnel-managed devices or workstations.

(904) *Physical security measures:* Alphabet must require the third-party OSE to implement appropriate physical security measures to protect systems and storage media used to store or process the Search Dataset against unauthorised physical access, removal, or tampering.

(905) *Logging, monitoring and accountability measures:* Alphabet must require the third-party OSE to:

(a) ensure that all access to the Search Dataset is logged, including attribution to individual users or systems and that such logs are protected against unauthorised access, alteration, or tampering, including through appropriate separation of duties;

[1158] The least-privilege principle means that personnel, systems, or processes are granted only the minimum level of access permissions necessary to perform their assigned functions.

[1159] The need-to-know principle means that authorised personnel who have been granted access rights may access data only when required for the performance of their assigned tasks.

(b) to retain access logs for a period of one year, in order to align with the audit requirement set out in section 4.4.4.2.4.1.1.

(906) *Data life cycle management*: Alphabet must require the third-party OSE to ensure that the Search Dataset is securely erased or rendered irrecoverable upon expiry of the 13 months retention period in accordance with recognised industry standards.

(907) *System security maintenance and vulnerability management*: Alphabet must require the third-party OSE to implement and maintain appropriate measures within the segregated processing environment to identify, assess, document, prioritise and timely remediate vulnerabilities and security weaknesses affecting systems, applications and authorised interfaces used to store, process or access the Search Dataset, with a view to preventing unauthorised access, disclosure, alteration or loss of the Search Dataset and maintaining the ongoing confidentiality, integrity and resilience of the segregated processing environment.

(908) *Data breach reporting:* Alphabet must require the third-party OSE to implement processes to detect, report, and respond to any actual data breach affecting the integrity or confidentiality of the Search Dataset in accordance with Article 33 and 34 of Regulation (EU) 2016/679.[1160]

(909) Alphabet may provide recommendations to the third-party OSE on the suitable technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset in line with the measures set out in this section.

4.4.4.2.3.2. The Commission's assessment

(910) The Commission considers that, to mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk vis-à-vis any other person, namely unintended third parties that are not eligible recipients of the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925, Alphabet must require third-party OSEs to comply with a set of contractual obligations, constituting the essential safeguards necessary to protect the integrity and confidentiality of the Search Dataset.[1161]

(911) Those measures correspond to generally recognised information security and data governance practices[1162] to ensure that the Search Dataset is protected against unauthorised or unlawful access, disclosure, alteration or loss, including risks arising from external malicious actors and from employees or subcontractors acting beyond their authorised roles or with malicious intent. Taken together, these organisational

---

1160 Article 33 of Regulation (EU) 2016/679 addresses the circumstances which give rise to a "*[n]otification of a personal data breach to the supervisory authority*" and Article 34 of that Regulation addresses the specific circumstances where a "*[c]ommunication of a personal data breach to the data subject*".

1161 See also Expert Report On Anonymisation, Doc ID […], section 6.2.

1162 See Article 32 of Regulation (EU) 2016/679 which requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including measures such as encryption, ensuring the confidentiality and integrity of processing systems, and processes for regularly testing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing. See also European Data Protection Board, *SME Data Protection Guide – Secure Personal Data*, identifying commonly used security measures such as encryption, access control, logging and monitoring, and physical security, available at: https://www.edpb.europa.eu/sme-data-protection-guide/home_en.
Comparable baseline safeguards are also reflected in widely recognised information-security standards such as ISO/IEC 27001 information security management standard and related guidance issued by European Union Agency for Cybersecurity (ENISA) on good practices for cybersecurity and information-security management, available at: https://www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance.

and technical measures form essential safeguards which reduce the likelihood that the Search Dataset could be accessed, extracted, or otherwise used by unintended recipients. Together with the technical measures, they further mitigate the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level of risk vis-à-vis any other person.[1163]

(912) **First**, *Technical protection of the Search Dataset* via encryption at rest and in transit using state-of-the-art encryption ensures that the Search Dataset remains unintelligible to unauthorised parties even in the event of system compromise, interception, or physical loss of storage media. The European Union Agency for Cybersecurity highlights cryptography is a vital part of cybersecurity[1164] and Regulation (EU) 2016/679 explicitly lists it among the technical and organisational measures that a controller must envisage to ensure a level of security appropriate to the risk.[1165] Encryption constitutes a foundational safeguard of information security preventing third parties from accessing data that could otherwise enable correlation or re-identification. By rendering data unusable without authorised cryptographic access, these measures materially reduce the residual risk that the Search Dataset could be exploited by unintended recipients (i.e., malicious actors) and thereby preserving effective anonymisation vis-à-vis those unintended recipients. The Commission further considers that appropriate cryptographic key management measures, including secure storage, access restriction, rotation and revocation of encryption keys, are necessary to ensure the continued effectiveness of the encryption measures and to prevent unauthorised access to the Search Dataset through compromise or misuse of encryption keys.[1166]

(913) **Second,** *access control and access governance* measures ensure that the Search Dataset is accessible only to authorised personnel and systems strictly necessary for the permitted purpose, preventing unauthorised internal or external access that could compromise the confidentiality of the Search Dataset, and thereby contribute to decrease further the risks of end users' re-identification from the Search Dataset. The implementation of least-privilege and need-to-know principles, periodic review and revocation of access rights, as well as phishing-resistant multi-factor authentication for employees with access to the Search Dataset ensures that only appropriately authorised personnel of the third-party OSE can process and interact with the Search Dataset. Furthermore, the Commission considers that since compliance with the contractual measures depends not only on technical measures but also on human conduct, enforceable confidentiality obligations and yearly training are necessary and proportionate organisational measure that helps prevent misuse, unauthorised access and breaches of the contractual measures by authorised personnel.[1167]

(914) **Third**, *data handling and other protection measures*, including the prohibition of copying, downloading or locally storing the Search Dataset on any other device, such as employee-managed devices or workstations, reduce the risk that employees could access, retain or process the Search Dataset outside the segregated processing environment. Such measures limit the possibility that employees, whether

---

1163 Joint Guidelines, Doc ID […], paragraph 185.

1164 European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography.

1165 Article 32(1)(a) of Regulation (EU) 2016/679 "Security of processing".

1166 This also addresses EDPB comment on the proposed measures of 5 May 2026, Doc ID […]paragraph 27.

1167 This is also in line with Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 588, which suggests that "*personnel training and supervision"* should be required. See Also, Alphabet's submission on contractual measures, 3 June 2026, Doc ID […]p.11.

intentionally or inadvertently, act beyond their authorised role by extracting data for purposes unrelated to the permitted processing or by transferring data into environments not subject to same safeguards.

(915) **Fourth**, *physical security measures* prevent unauthorised physical access to systems and storage media used to store or process such data. Appropriate physical safeguards therefore complement the data handling and other protection measures, as described in this section, by reducing the likelihood that the Search Dataset could be accessed or extracted outside authorised processes.

(916) **Fifth,** *logging, monitoring and accountability measures* ensure traceability and accountability for all access to the Search Dataset. Comprehensive logging, attribution of access to identifiable users (i.e., employees and other authorised personnel acting on behalf of the third-party OSE) or systems, and protection of logs against alteration or tampering create a deterrent effect against authorised personnel exceeding authorised access rights and enable the detection and investigation of anomalous or unauthorised behaviour. Retention of access logs for a minimum period of one year is appropriate for the annual audit and independent verification mechanism set out in section 4.4.4.2.4.1. In particular, retaining logs for at least the duration of the audit period ensures that auditors can verify compliance with authorised roles and permitted purposes of use, and investigate potential incidents that may only be identified after a delay. Such retention duration therefore enables *ex post* audits and verifications and, where necessary, corrective actions where access has occurred outside authorised roles or purposes, thereby reducing the residual risk of misuse or re-identification.

(917) **Sixth,** *data lifecycle management measures*, including the secure erasure or irreversible deletion of the Search Dataset upon expiry of the applicable retention period, limit the temporal scope within which the Search Dataset may be accessed or misused. By ensuring that the Search Dataset is not retained longer than necessary for the permitted purpose, these measures reduce opportunities for employees or other actors to access legacy datasets outside authorised operational needs and thereby further mitigate risks of unauthorised processing or re-identification over time.

(918) **Seventh**, the Commission considers it justified to specify a *system security maintenance and vulnerability management* measure. Effective protection of the Search Dataset requires not only reactive measures aimed at detecting, reporting and responding to data breaches as indicated below, but also proactive measures designed to identify and remediate vulnerabilities before they can be exploited. Requiring third-party OSEs to maintain processes for identifying, assessing, prioritising and timely remediating security weaknesses therefore complements the other technical and organisational safeguards specified in this Decision and contributes to maintaining the confidentiality, integrity and resilience of the segregated processing environment in which the Search Dataset is processed and maintained.

(919) **Eighth,** the *data breach reporting measure* ensures that third-party OSEs implement processes to detect, report and respond to data breaches in accordance with Article 33 and 34 of Regulation (EU) 2016/679. While these obligations already apply to all third-party OSEs in their capacity as controllers under Regulation (EU) 2016/679 in respect to the personal data forming part of the Search Dataset, the Commission considers it appropriate that Alphabet contractually require compliance with this measure so that they fall within the scope of the independent verification mechanism established in section 4.4.4.2.4.1. The Commission recalls that since a third-party

OSE is a separate controller for the processing of the Search Dataset insofar as it also contains personal data of other individuals, the responsibility for ensuring compliance with notification of a Search Dataset breach to the competent data protection supervisory authority and applicable communication of such a breach to the affected data subjects established under Articles 33 and 34 of Regulation (EU) 2016/679 lies with that OSE in accordance with the allocation of roles and responsibilities established in section 4.4.4.2.1.1. This approach guarantees that Search Dataset breaches are addressed in compliance with Union data protection law and in a verifiable manner, ensuring a high level of accountability for third-party OSEs accessing to the Search Dataset as a breach affecting the Search Dataset may not only affect the personal data of other individuals forming part of the Search Dataset but is also susceptible to increase the risks of end users' re-identification beyond an insignificant level depending on the circumstances of the breach.

(920) Alphabet claims that it has no right to be notified of data breaches, rendering the contractual framework ineffective.[1168] However, the Commission finds that the third-party OSEs must not be required to notify Alphabet of Search Data breaches since the independent verification mechanism set out in section 4.4.4.2.4 along Alphabet's ability to request an *ad hoc* audit (recital (1221)) and the expedited termination procedure (section 4.6.7.4) together provide an appropriate and proportionate framework in that regard.

(921) *In the first place*, the Commission considers that the independent verification mechanism set out in section 4.4.4.2.4 constitutes an appropriate and proportionate mechanism to assess whether Search Data breaches are handled in compliance with Regulation (EU) 2016/679 and whether the measures adopted in response thereto by the third-party OSE are appropriate. The mechanism ensures that the handling of such incidents is evaluated by an independent qualified practitioner possessing the necessary expertise and objectivity to determine whether the Search Data breaches reveal deficiencies in the third-party OSE's compliance with the contractual measures governing the integrity and confidentiality of the Search Dataset or not.

(922) Indeed, the mere occurrence of a Search Data breach does not, in itself, demonstrate that the third-party OSE failed to comply with the contractual measures or that the anonymisation of end users has been compromised. For example, a breach may result from the deliberate misconduct of an employee acting outside the scope of his/her authorised role, notwithstanding that the third-party OSE had implemented suitable technical, organisational and human controls to prevent such a conduct. Where such conduct is promptly detected, contained, remedied[1169] and reported in the third-party OSE's breach registry, the occurrence of the incident should not be considered as a deficiency in the third-party OSE's compliance with the contractual measures, nor would it necessarily create a material risk that end users could be re-identified. Quite the opposite, it could be considered that the third-party OSE has implemented, in accordance with Regulation (EU) 2016/679[1170] and its contractual obligation towards Alphabet, the required processes to detect, report and respond to Search Data breaches. Besides, a Search Data breach that is unlikely to result in any risk to the

---

1168 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 575, 577 and 588. See also Alphabet's submission on contractual measures, 3 June 2026, Doc ID […], p. 4 and 15.

1169 In such circumstances, the appropriate remediation may include the revocation of access rights or disciplinary measures against the employee as well as remediation of identified vulnerabilities by strengthening the relevant technical, organisational or human control to prevent further similar incident.

1170 Regulation (EU) 2016/679 would apply insofar as the breached data contains personal data (relating to other individuals than end users forming part of the Search Dataset), or at least insofar as the presence of such personal data cannot be excluded.

rights and freedoms of end users or other individuals, such as when the compromised data is unintelligible to unauthorised parties through strong encryption or secure hashing and the relevant keys remain intact, does not compromise end users' anonymisation.[1171] In this context, the independent verification mechanism is specifically designed to distinguish between isolated incidents that are appropriately detected, contained and remedied despite compliance with the contractual measures and incidents that reveal material deficiencies in the third-party OSE's compliance with those measures. It is only where such deficiencies are identified that they should be reflected in the conclusions of the assurance report issued by the independent qualified practitioner and trigger the suspension or termination of access to the Search Dataset as specified in sections 4.6.7.2 and 4.6.7.3.

(923) *In the second place,* the Commission considers that Alphabet's ability to request an *ad hoc* audit (recital (1221)) as well as to ensure expedited termination of access to Search Data (section 4.6.7.4) constitute timely, suitable and proportionate measures where objective evidence suggests that the integrity and confidentiality of the Search Dataset may have been materially compromised. Such evidence may arise, for example, where a third-party OSE is required to publicly communicate a personal data breach pursuant to Article 34 of Regulation (EU) 2016/679,[1172] or where Alphabet becomes aware that Search Data has been disclosed to unauthorised third persons, including through its appearance on publicly accessible sources or illicit online data marketplaces. In such circumstances, the existence of objective and verifiable evidence that the Search Dataset has escaped the controlled environment may justify Alphabet's request to conduct an *ad hoc* audit to verify the third-party OSE's continued compliance with the integrity and confidentiality contractual measures or the initiation by Alphabet of the expedited termination measure.

(924) *In the third place*, the Commission considers that a contractual obligation requiring third-party OSEs to notify Alphabet of all actual or suspected Search Data breaches would be disproportionate. In particular, the fact that a Search Dataset breach has been notified to the competent data protection supervisory authority in accordance with Article 33 of Regulation (EU) 2016/679 does not automatically mean that the third-party OSE has infringed its integrity and confidentiality obligations under that Regulation or corresponding contractual obligations towards Alphabet. Requiring the third-party OSE to notify Alphabet of Search Data breaches would effectively place Alphabet in a quasi-regulatory role, requiring it to evaluate the seriousness of incidents, the adequacy of containment and remediation measures, and the third-party OSE's ongoing compliance with its obligations. Such assessments are instead entrusted under Regulation (EU) 2016/679 to the competent supervisory authorities and, under the framework specified in this Decision, to the independent verification mechanism.

1171 EDPB Guidelines 9/2022 on personal data breach notification under GDPR version 2.0 of 28 March 2023, Section II "Article 33 – Notification to the Supervisory Authority", sub-section D. "Conditions where notification is not required", paragraphs 75-80.

1172 Article 34(1) of Regulation (EU) 2022/1925 provides that "[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subjects without undue delay". Article 34(3)(c) provides that in cases where such communication would involve a disproportionate effort "there shall be instead a public communication or similar measure whereby the data subjects are informed in an equally effective manner". Article 34(4) further provides that "[i]f the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require to do so (…)".

(925) *In the fourth place*, the Commission considers that a contractual requirement to notify Alphabet in cases of Search Data breaches could contradict access to Search Data on FRAND terms as required by Article 6(11) of Regulation (EU) 2022/1925. Indeed, such a requirement would create a risk that Alphabet could rely on the mere existence of a notified incident, irrespective of its severity, cause or remediation, as a basis to suspend or terminate access to the Search Dataset. However, as already explained above, the mere occurrence of a Search Data breach does not necessarily imply that the anonymisation of end users' personal data has been compromised or that the third-party OSE has failed to comply with the contractual measures. Given that individual Search Data breaches do not necessarily indicate non-compliance, risks for end users' anonymisation or reveal systemic deficiencies, requiring third-party OSE's to notify Alphabet of all such Search Data breaches would confer on it a disproportionate degree of control over third-party OSEs' continued access to Search Data.

(926) In light of the above, the Commission therefore considers that the combination of the independent verification mechanism, the possibility for Alphabet to request an *ad hoc* audit and the expedited termination procedure provides an appropriate and proportionate framework for addressing the risks for end users' anonymisation arising out of potential Search Data breaches. Within that framework, the handling and assessment of such breaches should primarily take place under Regulation (EU) 2016/679 and through the independent verification mechanism established by this Decision. Requiring notification of all Search Data breaches to Alphabet would therefore be neither necessary nor consistent with access on FRAND terms and allow Alphabet to use its procedural discretion to undermine contestability in online search.

(927) **Ninth**, The Commission considers that the contractual measures set out to ensure the integrity and confidentiality of the Search Dataset are appropriate and proportionate. Third-party OSEs process large volumes of data and, by the nature of their activities, already operate complex information systems exposed to cybersecurity and data protection risks. As a result, such undertakings are ordinarily required to implement appropriate technical and organisational security measures under existing Union and Member States law, including Regulation (EU) 2016/679 and, where applicable, Directive (EU) 2022/2555.[1173]

(928) **Finally**, the Commission disagrees with Alphabet's claim that the integrity and confidentiality measures would specify vague and open-ended security measures which significantly dilute the protection compared to Alphabet's Data Security Requirements[1174] applicable under the Google's licencing agreement as they would afford recipients with broad flexibility to determine their own measures.[1175]

(929) Indeed, the Commission considers that the specified measures correspond to widely recognised industry information security practices directly addressing the risks relevant to the processing of the Search Dataset, namely the risk of unauthorised or unlawful access of the Search Dataset by unintended recipients. They focus on core protections such as encryption of data at rest and in transit, strict access governance based on the principles of least privilege and need-to-know, secure data handling

---

1173 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, page 80-152.

1174 Alphabet's Data Security Requirements, available here: https://business.safety.google/datasecurityrequirements/. Doc ID […].

1175 Alphabet's response to Preliminary Findings, Doc ID [...], paragraphs 584-590.

practices, logging and monitoring of access, physical security protections, security maintenance and vulnerability management and data breach reporting.

(930) Besides, the specified measure in recital (909) provides that Alphabet may issue recommendations to the third-party OSE on the suitable technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset. Such recommendations may draw on Alphabet's experience in protecting large-scale search datasets and may constitute a useful reference point for third-party OSEs and independent auditors when assessing the suitability of technical, organisational and human controls implemented to ensure compliance with the specified integrity and confidentiality measures (recital (953)).

(931) However, the Commission considers that requiring compliance with a fixed set of security controls prescribed by Alphabet would not be appropriate in the present context.[1176] Instead, the Commission considers it is more appropriate for the legally binding measures specified in this Decision to remain principle-based security requirements aimed at ensuring the integrity and confidentiality of the Search Dataset, while allowing third-party OSEs, acting as independent controllers (see section 4.4.4.2.1), sufficient flexibility to determine the specific human, technical and organisational measures necessary to achieve those objectives in light of their own systems and risk environments. Third-party OSEs should remain free to implement alternative technical, organisation and human controls as long as they meet their integrity and confidentiality obligations as set out in section 4.4.4.2.3.1. It is not appropriate to require third-party OSEs to implement Alphabet's recommendations[1177] because such an approach would effectively allow Alphabet to determine, on an ongoing basis, the specific controls that third-party OSEs must adopt, thereby limiting their ability to implement alternative effective measures that take into account their own systems and risk environments. While Alphabet's recommendations may provide useful guidance, they should remain non-binding.

(932) Contrary to Alphabet's claim, the specified measures do not establish a static framework.[1178] The integrity and confidentiality measures require third-party OSEs to "*implement and maintain"* (emphasis added) appropriate controls arising from the processing of the Search Dataset and recognised industry standards for the protection of sensitive datasets, while the *system security maintenance and vulnerability management* measure requires third-party OSEs to adapt their safeguards to evolving security risks. The regular yearly audit will ensure that the safeguard put in place remain effective to meet all contractual requirements.

(933) In light of all the above, the Commission concludes that the set of contractual measures constituting the essential safeguards to protect the integrity and confidentiality of the Search Dataset, which Alphabet is required to impose on third-party OSEs, is proportionate. Together with the independent verification mechanism described below in section 4.4.4.2.4.1, these measures reduce the residual likelihood of end users' re-identification from the Search Dataset to an insignificant level vis-à-vis any other person (i.e. unintended third party that are not eligible recipients of the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925).

1176 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 584-590.

1177 Alphabet's response to the Revised Measures, 15 June 2026, Doc ID […], paragraph 117-118.

1178 Alphabet's response to the Revised Measures, 15 June 2026, Doc ID […]paragraph 118.

4.4.4.2.4. Independent verification mechanism to ensure the auditability and verifiability of anonymisation over time

(934) The Commission considers that, in the context of access to the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925, an independent verification mechanism - enabling the auditability and verifiability of contractual measures contributing to ensuring anonymisation over time - is justified and necessary. The mechanism must focus on an audit scope limited to systems relevant to the processing of the Search Dataset, with assurance objectives defined to enable effective independent verification that the contractual measures and eligibility criteria are met.

4.4.4.2.4.1. Measures

(935) Alphabet must require third-party OSE seeking access to the Search Dataset to provide an independent reasonable assurance report based on the audit scope and assurance objectives defined by the Commission throughout this section.

4.4.4.2.4.1.1. Independent reasonable assurance report

(936) Alphabet must require a third-party OSE seeking access to the Search Dataset, as a condition for obtaining and maintaining such access, to provide Alphabet with an independent assurance report providing reasonable assurance on the suitability and effectiveness of the controls implemented by the third-party OSE (also referred below as 'reasonable assurance report')[1179] to demonstrate compliance with the assurance objectives defined by the Commission in section 4.4.4.2.4.1.3 below (first[1180] second[1181] and third[1182] assurance objectives).

(937) The assurance reports must be prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, and must cover the organisational, technical, and governance measures implemented by the third-party

---

[1179] *International Framework for Assurance Engagements* issued by the International Auditing and Assurance Standards Board (IAASB), "Reasonable assurance engagements and limited assurance engagement", Doc ID 1885, page 45, paragraphs 14-16: available here: https://ifacweb.blob.core.windows.net/publicfiles/2024-08/IAASB-2023-2024-Handbook-Volume-4.pdf#page=46
A **reasonable assurance engagement** is defined as an assurance engagement in which the practitioner reduces assurance engagement risk to an acceptably low level in the circumstances of the engagement as the basis for a positive form of expression of the practitioner's conclusion. In practice, **reasonable assurance** therefore refers to a **high, but not absolute, level of assurance**, obtained by reducing engagement risk to an acceptably low level. This allows the practitioner to express a **positive conclusion** regarding whether the subject matter meets the applicable criteria.
By contrast, a **limited assurance engagement** is defined as an assurance engagement in which the practitioner reduces assurance engagement risk to a level that is acceptable in the circumstances of the engagement but where that risk is greater than for a reasonable assurance engagement, as the basis for a negative form of expression of the practitioner's conclusion. Accordingly, **limited assurance** provides a **lower level of assurance than reasonable assurance**, because less extensive procedures are performed and the risk is not reduced to a sufficiently low level to meet reasonable assurance. The practitioner therefore expresses a negative conclusion, typically stating that nothing has come to their attention that causes them to believe the subject matter is materially misstated.

[1180] The first assurance objective consists in verifying that the third-party online search engine has established credible and documented plans demonstrating that Search Data will be used for the genuine development, improvement, or optimisation of its own online search engine services.

[1181] The second assurance objective consists in verifying that the third-party online search engine has implemented effective technical, organisational, and contractual measures to ensure that Search Data is processed in compliance with the contractual obligations set out in section 4.4.4.2.2.1

[1182] The third assurance objective consists in verifying that the third-party online search engine has implemented effective technical, organisational, and contractual measures to protect the integrity and confidentiality of Search Data in compliance with the contractual obligations set out in 4.4.4.2.3.1

OSE in relation to the access, storage, processing, use, and protection of the Search Dataset received pursuant to Article 6(11) of Regulation (EU) 2022/1925, within the scope and in accordance with the three assurance objectives defined by the Commission in this section.

(938) The assurance reports must be issued by an independent assurance practitioner and must include a written signed declaration confirming the practitioner's independence, qualifications, experience and compliance with the ethical requirements applicable under ISAE 3000 or, where applicable, under an equivalent assurance framework, including requirements equivalent to those set out in the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA).

(939) As a condition for being granted initial access to the Search Dataset, Alphabet must require the third-party OSE to submit to Alphabet, in accordance with the conditions set out in section 4.6.6.1, a **Level 1 assurance report** prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, providing **reasonable assurance** on the first Commission-defined assurance objective as well as **on the design and suitability of the controls** put in place to meet the second and third Commission-defined assurance objectives.

(940) As a condition for maintaining access to the Search Dataset, Alphabet must require the third-party OSE to submit to Alphabet, on an annual basis and in accordance with the conditions set out in section (1218), a **Level 2 assurance report** prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, providing **reasonable assurance** on the first Commission-defined assurance objective as well as **on the operating effectiveness of those controls** and covering the Commission-defined assurance objectives. For the purposes of the Level 2 assurance report, the independent assurance practitioner must assess the operating effectiveness of the controls based on audit testing and sampling drawn from a continuous operating period of not less than 12 months within the reporting period, during which the controls were implemented and operational, with the exception of the first Level 2 assurance report which must be submitted on audit testing and sampling drawn from a continuous operating period of 3 months.

(941) Where the third-party OSE has obtained existing independent assurance reports, certifications, or audit reports (for example, ISAE 3000, ISAE 3402, SOC 2, ISO/IEC 27001, or equivalent), the auditor conducting the Level 1 or Level 2 engagement must take such reports into account, in whole or in part, when performing the engagement. In doing so, the auditor must ensure that:

(a) The scope, period, and assurance criteria of the existing reports demonstrably cover the Commission-defined assurance objectives;

(b) The reports cover the systems, environments, and organisational units within scope pursuant to section 4.4.4.2.4.1.2 ; and

(c) Any material gaps between the existing reports and the applicable assurance objectives are addressed through a targeted supplemental reasonable assurance engagement[1183].

[1183] In this context, the targeted supplemental reasonable assurance engagement means a reasonable assurance engagement, performed in accordance with applicable international assurance standards, that is limited in scope to specific controls or systems and carried out for the purpose of addressing material gaps between existing assurance reports, certifications, or audit reports and the assurance objectives defined by the Commission.

(942) The measures Alphabet must take regarding the submission of Level 1 and Level 2 assurance reports, the formal evaluation of those reports, and any resulting actions (including suspension of access, restoration of access or termination) in cases where the third-party OSE fails to provide a reasonable assurance report are set out in section 4.6.7.

4.4.4.2.4.1.2. Audit scope

(943) *Data scope:* the scope of the assurance engagement must be limited exclusively to the click, query, ranking and view data made available to the third-party OSE pursuant to Article 6(11) of Regulation (EU) 2022/1925 (the Search Dataset), including any datasets, models or outputs directly derived from such Search Dataset within the segregated processing environment. The assurance engagement must assess the implementation and effectiveness of measures protecting the Search Dataset, as required under the contractual obligations in sections 4.4.4.2.2 and 4.4.4.2.3.

(944) *Organisational scope*: the assurance engagement must cover only those parts of the third-party OSE's organisation that process, access, store, or otherwise handle the Search Dataset, including:

(a) the relevant business units, teams, and personnel with authorised access;

(b) internal governance, compliance, and oversight functions responsible for ensuring compliance with contractual obligations relating to the use, security, and anonymisation of the Search Dataset; and

(c) any subcontractors or internal service providers involved in processing the Search Dataset on behalf of the third-party OSE; and

(d) where necessary to achieve the assurance objectives organisational units and personnel responsible for planning, budgeting, and allocating resources or financial commitments directly associated with the development, improvement, or optimisation of the search engine using the Search Dataset.

(945) Organisational units, systems, or personnel that do not have physical, logical, or administrative access to the Search Dataset or whose financial or resource activities are unrelated to the Search Dataset processing must be excluded, provided that effective segregation is demonstrably implemented and maintained.

(946) *Technical scope*: the assurance engagement must cover all technical systems, environments, and controls used to:

(a) access or receive the Search Dataset from Alphabet;

(b) store, process, or otherwise handle the Search Dataset, including backup and recovery systems;

(c) analyse the Search Dataset or generate outputs, models, or derived datasets based on the Search Dataset; and

(d) manage, monitor, and log access to the Search Dataset.

(947) This includes, where applicable, cloud-based and on-premises environments, development, testing, and production systems in which the Search Dataset is present, as well as identity and access management systems, network security controls, and monitoring and logging systems relevant to the enforcement of contractual obligations for integrity, confidentiality, and continued anonymisation of the Search Dataset.

(948) Where reliance is placed on existing assurance reports, the assurance engagement may be limited to a mapping and gap assessment demonstrating how the controls and findings in such reports apply to the Search Dataset and any directly derived datasets or models.

4.4.4.2.4.1.3. Assurance objectives

(949) The assurance engagement must evaluate whether the third-party OSE satisfies the conditions applicable to the provision and use of the Search Dataset. In particular, the auditor must assess whether:

(a) the third-party OSE has established credible and documented plans demonstrating that the Search Dataset will be used for the genuine development, improvement, or optimisation of its own OSE services (First assurance objective);

(b) the third-party OSE has implemented effective technical, organisational, and contractual measures to ensure that the Search Dataset is processed in compliance with the contractual obligations set out in section 4.4.4.2.2.1 (Second assurance objective); and

(c) the third-party OSE has implemented effective technical, organisational, and contractual measures to protect the integrity and confidentiality of the Search Dataset in compliance with the contractual obligations set out in 4.4.4.2.3.1 (Third assurance objective).

(950) **First**, the auditor must verify whether the third-party OSE has established and maintains credible and documented plans, governance arrangements, and resource commitments demonstrating that the Search Dataset accessed pursuant to Article 6(11) of Regulation (EU) 2022/1925 will be and/or is used for the genuine development, improvement, or optimisation of its own OSE services, in line with the permitted purposes of use and without undermining anonymisation measures. This objective is assessed by verifying:

(a) documented investment planning and financial commitments, including the existence of formal investment plans, budgets, or strategic programmes approved by senior management that allocate dedicated resources to the development or improvement of the third-party OSE's own search technology, and that clearly identify how, and for which development activities, the Search Dataset accessed pursuant to Article 6(11) of Regulation (EU) 2022/1925 is intended to be used for optimising OSE services.

(b) credibility of investment plans, including evidence that planned investments, budgets, or strategic programmes are genuine and realistic in scale, timeframe, and scope relative to the stated development objectives.

(c) adequacy of resourcing for implementing or preserving anonymisation-of the Search Dataset.

(d) that the third-party OSE only serves search results generated by its own search algorithms and technologies and does not merely copy search results directly from the Search Dataset.

(951) **Second**, the auditor must verify that the third-party OSE has implemented effective measures contributing to ensuring anonymisation of the Search Dataset over time. This objective is assessed by verifying the suitability and effectiveness of technical, organisational, and human controls in the following areas:

(a) Ensuring that the Search Dataset is maintained within a processing environment under the effective control of the third-party OSE and that any processing of the Search Dataset by the third-party OSE or its subcontractors take place only within that processing environment.

(b) Ensuring that the Search Dataset is maintained exclusively within a logically and technically segregated processing environment and that processing of the Search Dataset by the third-party OSE and its subcontractors is confined to that environment, such that the Search Dataset cannot be linked with any auxiliary dataset accessible to the third-party OSE or its subcontractors. In particular, technical and organisational controls must effectively prevent the Search Dataset from:

  (1) being queried jointly with auxiliary datasets;

  (2) being copied, merged, synchronised across the third party OSE's systems with auxiliary datasets;

(c) Ensuring that the Search Dataset is used solely for the permitted purposes of use of optimising or improving OSE services as specified in recital (822) and is not processed for unrelated purposes.

(d) Preventing, detecting and responding to any attempts, whether intentional or incidental, to:

  (1) link the Search Dataset with auxiliary datasets at record level;

  (2) re-identify end users, including by attempting to determine, learn or annotate which records relate to the same end user (i.e. re-sessionisation), in any way such as semantic similarity, behavioural fingerprinting or other techniques beyond any mini-sessionisation provided as part of the Search Dataset; or

  (3) augment, enhance, or process the Search Dataset in a manner that reverses, weakens, or circumvents applied technical anonymisation measures, including attempts to infer or reconstruct generalised, truncated, or removed attributes.[1184]

(e) Ensuring that the third-party OSE conducts and documents pre-deployment evaluation of the machine learning models, including models supporting ranking, retrieval, or AI chatbot functionalities that were trained with the Search Dataset model to verify that it does not, under reasonably foreseeable inputs, reproduce data from the Search Dataset in a manner exposing end users to risks of re-identification.

(f) Preventing, detecting and responding to any unauthorised disclosure, sharing, sublicensing, or other making available of the Search Dataset to third parties.

(g) Maintains accurate and up-to-date documentation of automated systems and processes accessing the Search Dataset, material processing operations involving the Search Dataset and models trained or fine-tuned using the Search Dataset that are subject to the testing safeguard provided for in recital (825) and testing results in a manner that enables verification that the processing complies with the contractual prohibitions and remains aligned with the permitted uses.

[1184] Data enrichment is permitted if it is limited to transformations that do not increase the risk of re-identification.

(952) **Third**, the auditor must verify that the measures implemented by the third-party OSE are designed to protect the integrity and confidentiality of the Search Dataset against unauthorised access, disclosure, alteration, or loss, including in the event of internal misuse or external compromise. This objective is assessed by verifying the suitability and effectiveness of technical, organisational, and human controls in the following areas:

(a) Ensuring that the Search Dataset is encrypted when stored or transmitted between systems or environments under the third-party OSE's control, using state-of-the-art encryption appropriate to the sensitivity of the data and the risks it is intended to mitigate, including unauthorised access resulting from physical loss or theft of storage media, and that appropriate cryptographic key management measures are implemented, including secure storage, access restriction, rotation and revocation of encryption keys.

(b) Restricting access to the Search Dataset to authorised personnel and systems strictly necessary for the permitted purpose and assigning access rights in accordance with the principles of least privilege and need-to-know, with periodic review and revocation of access rights where access is no longer necessary.

(c) Requiring authorised personnel with access to use phishing-resistant multi-factor authentication.

(d) Ensuing that authorised personnel with access to the Search Dataset are subject to enforceable confidentiality obligations and receive yearly training regarding access restrictions, secure handling requirements, authorised and prohibited uses of the Search Dataset, and applicable governance and traceability obligations.

(e) Prohibiting the copying, downloading, or local storage of the Search Dataset on any other device, including personnel-managed devices or workstations.

(f) Implementing appropriate physical security measures to protect systems and storage media used to store or process the Search Dataset against unauthorised physical access, removal, or tampering.

(g) Ensuring that all access to the Search Dataset is logged and monitored~~,~~ including attribution to individual users or systems, and that such logs are protected against unauthorised access, alteration, or tampering, including through appropriate separation of duties, and retained for a period of one year enabling independent audit.

(h) Ensuring that appropriate measures are implemented and maintained to identify, assess, document, prioritise and timely remediate vulnerabilities and security weaknesses affecting systems, applications and authorised interfaces used to store, process or access the Search Dataset, with a view to preventing unauthorised access, disclosure, alteration or loss of the Search Dataset and maintaining the confidentiality, integrity and resilience of the segregated processing environment.

(i) Ensuring that the Search Dataset is securely erased or rendered irrecoverable upon expiry of the 13 months applicable retention period, in accordance with recognised industry standards

(j) Ensuring that robust, documented and auditable processes are implemented to detect, assess, report, and respond to actual or suspected data breaches

affecting the integrity or confidentiality of the Search Dataset in accordance with Articles 33 and 34 of Regulation (EU) 2016/679. The auditor shall verify that:

(1) Appropriate policies, procedures, and controls are established and implemented to ensure the timely detection, escalation, assessment, notification and where required, communication of data breaches within the applicable deadlines;

(2) All data breaches are systematically recorded in a breach register, including the facts relating to the breach, its effects, and the remedial actions taken;

(3) Sufficient and traceable evidence (including logs, incident reports, communications, and post-incident reviews) is retained to allow *ex post* verification of compliance.

(953) The auditor can take into account Alphabet's recommendations regarding the technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset when assessing the suitability and effectiveness of the third-party OSE's controls.

4.4.4.2.4.2. The Commission's assessment

(954) The Commission considers that, in the context of access to the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925, an independent verification mechanism - enabling the auditability and verifiability of contractual measures contributing to ensuring anonymisation over time - is justified and necessary. The mechanism should focus on an audit scope limited to systems relevant to the processing of the Search Dataset, with assurance objectives designed to enable effective independent verification that the contractual measures and eligibility criteria are met.

4.4.4.2.4.2.1. An independent verification mechanism is justified and necessary

(955) **First**, the Commission considers that, in the context of access to the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925, an independent verification mechanism enabling the auditability and verifiability of contractual measures contributing to ensuring anonymisation over time is justified and necessary to ensure that the likelihood of re-identification remains insignificant throughout the duration of access and processing of the Search Dataset.[1185]

(956) Indeed, once the Search Dataset is accessed and processed outside Alphabet's technical environment, the continued effectiveness of anonymisation depends, in addition to the technical measures bringing the risk to a residual level, on complementary organisational, technical, and governance measures implemented by third-party OSEs.

(957) In this context, a verification mechanism is necessary to ensure that those measures remain suitable and effective in preventing re-identification risks, including risks arising from the combination of the Search Dataset with auxiliary datasets. Such a verification mechanism is necessary and justified to ensure transparency, accountability and trust in the data-sharing framework and ensures that compliance with the contractual measures can be objectively demonstrated and assessed throughout the duration of access.

[1185] Joint Guidelines, Doc ID […], paragraph 181.

(958) **Second**, the Commission finds that the assurance mechanism must be based on independent assurance.

(959) *On the one hand***,** reliance on audits conducted or substantively controlled by Alphabet cannot provide sufficient objectivity and impartiality. Alphabet's current Data Security Requirements provides that "*upon request by Google, Google may conduct, via an independent auditor of Google's selection, audits of Recipient's architecture, systems, processes, and procedures relevant to the protection of Protection Information*." While such a clause may serve legitimate purposes in the context of Alphabet's internal security and contractual risk management, it is not appropriate in the present context. In particular, the selection, mandate and scope of the audit would remain under the control of Alphabet, which is the designated gatekeeper subject to the obligation to share the Search Dataset with third-party OSEs. Given that the objective of that obligation is to enable those undertakings to contest the position of Google Search, a verification mechanism controlled or substantially influenced by Alphabet would create a structural conflict of interest and could undermine the fairness and neutrality of the verification process.

(960) *On the other hand*, reliance on self-attestation by third-party OSEs would likewise fail to provide an objective or verifiable assessment of compliance with the anonymisation, integrity, and confidentiality contractual measures. Self-attestation lacks independent oversight and would rely solely on the representations of the third-party OSE, which may have incentives to interpret the contractual measures in a manner favourable to its own operational needs. Such an approach would therefore not provide sufficient assurances that the relevant organisational, technical and governance measures are effectively implemented and maintained over time, nor that potential weaknesses or deviations would be detected and addressed in a timely manner.

(961) As a result, the Commission is of the view that only an independent assurance mechanism, performed by qualified practitioners applying recognised professional assurance standards, ensures that compliance is assessed impartially and on the basis of objective evidence according to established professional methodologies. It also ensures that the contractual measures remain auditable, verifiable, and transparent to Alphabet, the Commission, and, indirectly, to end users whose rights to private life and protection of personal data are safeguarded by the anonymisation requirement enshrined in Article 6(11) of Regulation (EU) 2022/1925.

(962) **Third**, the Commission considers that assurance engagements conducted in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework constitute an appropriate and proportionate means of verifying compliance with the assurance objectives set out in section 4.4.4.2.4.1.3. The choice of such a framework is based on the following considerations.

(963) The Commission examined whether requiring ISO/IEC/27001 certification could constitute an appropriate pre-condition for access to the Search Dataset. However, in light of the consistent feedback from potential beneficiaries, the Commission considers that such a requirement would be disproportionate. Those beneficiaries highlighted that ISO/IEC/27001 certification could lead to duplicative compliance burdens for entities already subject to other applicable security or cybersecurity frameworks and could entail significant financial, administrative and time-related costs, in particular on smaller or emerging third-party OSEs, thereby risking to

exclude from access to the Search Dataset those undertakings that Article 6(11) of Regulation (EU) 2022/1925 seeks to enable.[1186]

(964) By contrast, the Commission considers that the alternative ISAE 3000 framework or an equivalent internationally recognised framework is suitable for assessing compliance with the assurance objectives in the present context, as confirmed by experienced assurance practitioners.[1187]

(965) While ISO/IEC 27001 focuses on the establishment and certification of an information security management system, ISAE 3000 provides a principles-based assurance framework that can be tailored to the specific subject matter at hand, including not only integrity and confidentiality controls but also safeguards relating to anonymisation and the mitigation of re-identification risks as well as verification of investment plans. This makes it particularly appropriate for assessing the three Commission-defined assurance objectives detailed in section 4.4.4.2.4.1.3.

(966) In addition, and contrary to Alphabets' claim,[1188] assurance engagements under ISAE 3000 do not only attest to the existence of policies or controls at a point in time, but also provide assurance on the design, implementation and operating effectiveness of controls over a defined period. It follows that such engagements enable a comprehensive assessment of whether the relevant safeguards and controls are effectively applied in practice, thereby providing a high level of confidence in the ongoing compliance of third-party OSEs with the applicable contractual measures they are subject to when accessing and processing the Search Dataset. This has also been confirmed by experienced assurance practitioners.[1189]

(967) Finally, ISAE 3000 or equivalent internationally recognised assurance frameworks provide sufficient flexibility for each third-party OSE to implement organisational and technical controls tailored to its specific risk environment and operational profile. This flexibility allows OSEs to take into account existing compliance frameworks and security arrangements already in place, and to adopt different approaches to meet the assurance objectives, provided that they can demonstrate, through the assurance engagement, that those objectives are effectively met.

(968) **Fourth**, the Commission considers that independent assurance must be performed by qualified practitioners applying recognised professional assurance standards and complying with the relevant ethical requirements. In this regard, requiring practitioners to comply with the ethical requirements applicable under ISAE 3000, including those equivalent to the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA),[1190] ensures that assurance engagements are conducted in accordance with recognised principles of professional integrity, objectivity, professional competence and independence. These

---

1186 [Market participant]'s reply to RFI of 18 November 2025, Doc ID […], question 16, page 11; [market participant]'s reply to RFI of 18 November 2025, Doc ID […], question 16, page 16; [market participant]'s response to RFI of 18 November 2025, Tranche 1, Doc ID […], question 16, page 7; [market participant]'s reply to RFI of 18 November 2025, Doc ID […], question 16, page 14.

1187 Minutes of meeting with [audit firm]of 7 January 2026, Doc ID […]; Minutes of meeting with [audit firm] of 13 January 2026, Doc ID […]; Minutes of meeting with [audit firm]of 22 January 2026, Doc ID […].

1188 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 576 a).

1189 Minutes of meeting with [audit firm]of 7 January 2026, Doc ID […]; Minutes of meeting with [audit firm]of 13 January 2026, Doc ID […]; Minutes of meeting with [audit firm]of 22 January 2026, Doc ID […].

1190 See the International Code of Ethics for Professional Accountants here: https://www.ethicsboard.org/iesba-code

ethical safeguards are essential to ensure that the practitioner's assessment is free from conflicts of interest and undue influence from the audited third-party OSE.

(969) **Fifth**, the Commission considers that an initial assurance report (Level 1 or similar) ensures that appropriate safeguards are in place prior to granting access to the Search Dataset, while yearly assurance reports (Level 2) ensure that those safeguards remain effectively implemented in practice and continue to achieve the assurance objectives during the period of access and processing of the Search Dataset. This two-step approach reflects established assurance practices, as confirmed by experienced assurance practitioners,[1191] and ensure that anonymisation measures do not deteriorate over time due to changes in systems, processing practices or organisational arrangements by the third-party OSEs. Consistent with established assurance practices, the independent auditor assesses whether the safeguards implemented by the third-party OSE are sufficient to meet the applicable assurance objectives and, where appropriate, may identify deficiencies or recommend additional controls or measures to ensure that those objectives continue to be met.[1192]

(970) Besides, the annual frequency aligns with established international assurance practices. For example, ISO/IEC 27001 requires surveillance audits at least once per year to verify that controls remain effective and that the management system continues to comply with the standard's requirements.[1193] This frequency is also proportionate: it is appropriate to detect changes or deficiencies in systems, processing practices, or organisational arrangements by the third-party OSEs, without imposing an undue administrative burden.

(971) **Sixth**, the Commission considers that all existing independent assurance reports, certifications or audit reports obtained by third-party OSEs must be taken into account where they demonstrably cover the relevant assurance objectives. This approach ensures proportionality by avoiding unnecessary duplication of audits and limiting additional compliance burdens to what is necessary to address any gaps between existing assurance frameworks and the assurance objectives defined by the Commission in section 4.4.4.2.4.1.3. Experienced assurance practitioners consulted by the Commission have also confirmed that this is a sensible approach.[1194]

(972) **Seventh**, as already outlined in recital (927), third-party OSEs process large volumes of data and, by the nature of their activities, already operate complex information systems exposed to cybersecurity and data protection risks. As a result, such undertakings are ordinarily required to implement appropriate technical and organisational security measures under existing Union and Member States law, including Regulation (EU) 2016/679 and, where applicable, Directive (EU) 2022/2555. In that context, the Commission considers that the contractual measures set out to ensure that the third-party OSEs are subject to an independent verification mechanism is appropriate and proportionate.

1191 Minutes of meeting with [audit firm]of 13 January 2026, Doc ID […]; Minutes of meeting with [audit firm]of 7 January 2026, Doc ID […].

1192 *Idem*.

1193 ISO/IEC 27001 certifications are subject to a three-year cycle including mandatory annual surveillance audits to verify the continued effectiveness and compliance of the Information Security Management System.

1194 Minutes of meeting with [audit firm]of 7 January 2026, Doc ID […]; Minutes of meeting with [audit firm] of 13 January 2026, Doc ID […]; Minutes of meeting with [audit firm]of 22 January 2026 Doc ID […].

(973) **Finally**, the Commission rejects Alphabet's characterisation of the independent verification mechanism as a "box-ticking exercise" that does not provide for appropriate means to detect breaches of contractual measures.[1195]

(974) *In the first place,* such a characterisation is difficult to reconcile with the widespread reliance placed by the Union legislature and regulators on independent audit, assurance engagements, certifications and conformity assessments as tools to assess and verify compliance in complex technical environments.[1196] Alphabet itself relies on independent audits, certifications and assurance reports to provide customers and business partners with confidence regarding the effectiveness of its own controls.[1197] The Commission therefore does not accept Alphabet's suggestion that an assurance engagement conducted by independent qualified practitioners in accordance with a recognised professional standard such as ISAE 3000 would amount to a mere box-ticking exercise devoid of evidential value.

(975) *In the second place*, the Commission considers that the independent verification mechanism set out in this section 4.4.4.2.4 provide for the appropriate means to detect breaches of contractual measures. In this regard, the Commission notes that it is not necessary for the assurance mechanism to guarantee the detection of every conceivable breach in order to be effective. The relevant question is whether the mechanism provides a reasonable, regular, and independent means of verifying that third-party OSEs demonstrate that suitable technical, organisational and human controls are effectively applied in practice thereby providing a high level of confidence in the ongoing compliance of third-party OSEs with the applicable contractual measures. The Commission considers that the independent assurance mechanism achieves that objective.

4.4.4.2.4.2.2. The audit scope is limited to systems that are relevant to the processing of the Search Dataset

(976) The Commission considers that the scope of the assurance engagement must be clearly limited to the data, organisational units, and technical systems, and where relevant, financial and resource allocations that are directly associated with the processing of the Search Dataset under Article 6(11) of Regulation (EU) 2022/1925. This limitation ensures that the auditor's assessment remains focused on the contractual measures governing access to and use of and investment in Search Data. This is also supported by several third-party OSEs.[1198]

1195 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 575-578.

1196 See for instance Articles 37 to 39 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *OJ* L 277, 27.10.2022, which establish a regime of independent audits for very large online platforms and very large online search engines.

1197 See Google Cloud and SOC 2 compliance webpage, https://cloud.google.com/security/compliance/soc-2?hl=en&utm_source=chatgpt.com#google-cloud-and-soc-2-compliance (last accessed 11/06/2026): "*Google Cloud regularly undergoes third-party audits for our products, systems, and infrastructure related to this standard. The SOC 2 reports are generated by an objective third party attesting to a set of assertions made by Google Cloud about its controls that are in place to protect customer data. The audit firm's evaluation includes comprehensive testing of the design and operating effectiveness of the controls within the audit period. Customers may use the SOC 2 report to assess the risks arising from interactions with the assessed Google Cloud and Google Workspace systems throughout the period*."

1198 [Market partciipant]'s reply to RFI of 16 January 2026, Doc ID […], question 12, page 7; [market participant]'s reply to RFI of 16 January 2026, Tranche 1, Doc ID […], question 12; [market participant]'s reply to RFI of 16 January 2026, Doc ID […], question 12, page 8; [market participant]'s reply to RFI of 16 January 2026, Doc ID […], question 12, page 7.

(977) Regarding the data scope, the Commission considers that limiting the scope to the Search Dataset and datasets, models, or outputs directly derived from the Search Dataset ensures that the assurance engagement focuses on the risks arising from the subsequent processing of the Search Dataset, while avoiding an extension of the engagement to unrelated processing activities of the third-party OSE.

(978) Regarding the organisational scope, the Commission finds that it must be focused on organisational units, personnel, and governance functions that actively process, access, or allocate resources to the Search Dataset, ensuring that both operational and resource-related aspects of data processing are properly managed. This includes financial records, investment plans, budgets, and other resource allocations directly supporting the development, improvement, or optimisation of the search engine services using the Search Dataset. Organisational units, personnel, or financial/resource activities unrelated to the Search Dataset should be explicitly excluded where effective segregation measures are demonstrably implemented, thereby maintaining a targeted and proportionate audit scope.

(979) Regarding technical scope, the Commission finds that it must focus on systems, environments and controls that process or have access to the Search Dataset. This includes systems used to access, analyse, or generate outputs, models, or derived datasets from the Search Dataset, as well as technical controls for monitoring, logging, and securing data. Systems or environments without physical, logical, or administrative access to the Search Dataset, where effective segregation measures are demonstrably implemented, are explicitly excluded to ensure the audit scope remains targeted on components that can materially affect the integrity, confidentiality, or anonymisation of the Search Dataset.

(980) As explained in recital (971), the Commission also considers it necessary to structure the assurance engagement in a manner that avoids duplication of existing assurance activities and thereby limits unnecessary administrative and financial burden for third-party OSEs. Accordingly, where reliance is placed on existing assurance reports, the engagement may be limited to a mapping and gap assessment, provided that such assessment enables verification that the controls and findings covered by those reports adequately address the risks and contractual obligations associated with the processing of the Search Dataset, and provide a sufficient basis for independent verification of compliance.

4.4.4.2.4.2.3. The Commission defined assurance objectives are relevant to enable effective independent verification that the contractual measures and eligibility criteria are met

(981) The Commission considers that the assurance objectives must be defined to enable effective independent verification that third-party OSEs accessing the Search Dataset pursuant to Article 6(11) of Regulation (EU) 2022/1925 both satisfy certain eligibility requirements and implement the contractual measures governing access to and processing of the Search Dataset while ensuring that the assurance engagement remains targeted and proportionate.

(982) The assurance objectives are defined by the Commission to ensure that independent verification is both fair and credible. If the Gatekeeper defined the objectives, they could be set too broadly, creating unnecessary burdens, while if a third-party OSE defined them, they could be too narrow. By establishing the assurance objectives, the Commission ensures that all third-party OSEs are assessed against the same clear and proportionate criteria to ensure access to the Search Dataset on FRAND terms, while protecting the independence of the assurance engagement.

(983) The assurance objectives are designed to: (i) assess whether credible and documented investment plans, governance arrangements, and resource commitments exist to ensure that the Search Dataset is used solely for the genuine development, improvement, or optimisation of the third-party OSE's own search technology and services; (ii) verify that effective measures are in place to preserve the anonymisation of the Search Dataset over time; and (iii) verify that effective measures protect the integrity and confidentiality of the Search Dataset.

(984) The first objective is to verify that the third-party OSE has established and maintains credible and documented plans, governance arrangements, and resource commitments demonstrating that the Search Dataset is used solely for the genuine development, improvement, or optimisation of its own online search technology and related services. This includes assessing the existence and credibility of documented investment plans or strategic programmes, the execution of prior commitments where applicable and the adequacy of allocated resources. The existence of such credible plans, governance arrangements and resource commitments are evidence demonstrating that the third-party OSE in question plans to develop its OSE as a genuine business and to contest Alphabet's position in the OSE CPS. Lack of such credible documentation may indicate a risk that the Search Dataset could be used for purposes other than optimising an OSE, which is not permitted under Article 6(11) of Regulation (EU) 2022/1925.

(985) The execution of prior commitments is also an indicator of the credibility of future plans and resource commitments. For instance, if a third-party OSE has committed investment and hired or assigned staff to further optimise its OSE, this indicates that its future plans to use Search Data for the purpose of optimising an OSE are credible.

(986) Moreover, independent verification that the third-party OSE only serves search results generated by its own search algorithms and technologies rather than merely copying results directly from the Search Dataset is necessary to ensure that third-party OSEs adhere to the *permitted purposes of use* specified in recital (822). Direct copying of Alphabet's search results and algorithms is expressly outside these permitted purposes of use measure, which states that Alphabet shall require the third-party OSE to use the Search Dataset solely for the permitted purposes of use of optimising or improving OSE services. This means, in effect, that the auditor should verify that the third-party OSE does not use the Search Dataset as a lookup table, merely copying results directly from the Search Dataset.

(987) The second and third assurance objectives are defined so as to mirror the contractual measures set out in sections 4.4.4.2.2.1 and 4.4.4.2.3.1. This approach ensures a clear and verifiable link between the contractual obligations imposed on the third-party OSE, the controls subject to audit in line with its scope, and the conclusions reached in the independent assurance report. By structuring the assurance objectives in this manner, the engagement enables the auditor to assess whether the contractual measures are effectively implemented and operate as intended.

(988) More specifically, the second objective is to verify that the third-party OSE has implemented effective measures to ensure anonymisation of the Search Dataset over time. The assessment focuses on whether the Search Dataset is maintained in a segregated processing environment under the effective control of third-party OSE, whether it is used solely for the permitted purposes of use, whether attempts to link, re-identify, or otherwise circumvent anonymisation safeguards are prevented whether unauthorised disclosure to third-party is prevented, and whether downstream datasets, and automated processes are appropriately documented to support

verification of compliance with contractual measures ensuring anonymisation from the perspective of the third-party OSE.

(989) The third objective is to verify that measures have been implemented to protect the integrity and confidentiality of the Search Dataset against unauthorised access, disclosure, alteration, or loss, including in cases of internal misuse or external compromise. The auditor assesses the suitability and effectiveness of technical, organisational, and human controls such as encryption, access controls, authentication, physical security, logging and monitoring, secure erasure, and data breach detection and response, to ensure that the Search Dataset is appropriately safeguarded throughout its lifecycle. As explained in recitals (930) and (931), the auditor can take into account, as a reference point, Alphabet's recommendations regarding the technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset when assessing the suitability and effectiveness of the third-party OSE's controls. However, as those recommendations remain non-binding, the third-party OSE is not obliged to follow them and may adopt alternative measures and controls, provided that it can demonstrate that such measures controls ensures the integrity and confidentiality of the Search Dataset.

(990) At the same time, in accordance with the audit scope defined in section 4.4.4.2.4.1.2, the second and third assurance objectives are limited to those elements necessary to assess compliance with the contractual obligations applicable to the Search Dataset and to datasets, models, or outputs directly derived from such data. The Commission considers such limitation necessary to ensure that the assurance engagement remains limited to the specific risks arising from the sharing and processing of the Search Dataset and does not evolve into a broader assessment of the third-party OSE's general data governance, security, or compliance framework.

4.4.5. Conclusions

(991) The Commission concludes that the technical measures that Alphabet must implement and the contractual measures that Alphabet must require in its contractual arrangements with third-party OSEs, taken together, ensure that the likelihood of end users' re-identification is, from the perspective of third-party OSEs or any other third person, insignificant. Therefore, the Commission concludes that the technical and contractual measures that Alphabet must implement ensure anonymisation of end users' personal data while preserving data quality and usefulness for third-party OSEs and thereby ensure an effective implementation of Article 6(11) of Regulation (EU) 2022/1925.

4.5. Measures relating to the FRAND pricing of Alphabet's Search Data

4.5.1. Introduction

(992) As laid down in Article 6(11) of Regulation (EU) 2022/1925, Alphabet must provide access to relevant Search Data on FRAND terms. The price at which eligible beneficiaries may access Search Data is part of those terms and must therefore be FRAND.

(993) In the following sections, the Commission first reviews Alphabet's current pricing offer and approach for providing access to the Search Data and presents its views; then it presents the views expressed by third parties, including those that may qualify as eligible beneficiaries; and finally it clarifies the interpretation of FRAND in the context of Article 6(11) of Regulation (EU) 2022/1925 and specifies the approach Alphabet must follow to establish its FRAND pricing strategy for providing access to the Search Data.

(994) The Commission considers that the FRAND nature of the pricing measures specified under Article 6(11) of Regulation (EU) 2022/1925 should be assessed in light of the specific objectives of that provision, the broader objectives of fairness and contestability, and the specific circumstances in which the pricing measures are specified, including the position of the beneficiaries relative to Alphabet, their scale in the provision of online search services, and the bounded time during which they may benefit from such data sharing. As further developed in section 4.5.3 below, the Commission concludes that FRAND pricing terms under Article 6(11) of Regulation (EU) 2022/1925 should enable eligible beneficiaries to effectively access the Search Data to optimise their search services, without preventing Alphabet from continuing to provide its own search services, and thus specifies that a cost-based approach, which provides Alphabet with a fair chance to cover the incremental cost of providing access to the Search Data and to obtain a reasonable return on capital employed for that purpose, is the appropriate approach to establish pricing terms that can be considered FRAND under Article 6(11) of Regulation (EU) 2022/1925. The Commission further specifies that only under certain circumstances, it may be justified to depart from this approach to ensure such FRAND nature of the measures.

4.5.1.1. Alphabet's approach and pricing offer

(995) Alphabet maintains that FRAND is an overall range of commercial outcomes rather than a specific price based on benchmarks,[1199] and that reasonableness is determined by the commercial value rather than by internal costs.[1200]

(996) Alphabet notes that it is universally recognised that FRAND pricing is assessed by reference to the *intrinsic value* of the data shared.[1201] Alphabet claims that this is unanimously supported by applicable precedents and EU legislation, and that it constitutes the industry best practice in the Standard Essential Patent ("SEP") valuation context. [1202] Alphabet further claims that, according to the case law, the legally correct and economically rigorous methodology to establish such value-based FRAND pricing is to rely on benchmarks based on a comparable service existing in a competitive market.[1203] According to Alphabet, because of the novelty and the high value offered by its Search Data, any proposed benchmark is conservative and can only serve as a floor for the price of its Search Data.[1204] Alphabet also suggests that the price for its Search Data could alternatively be assessed by considering the investment savings for the recipients.[1205]

(997) According to Alphabet, a cost-based approach is not FRAND, would by nature deprive the Search Data of its value,[1206] and be expropriatory.[1207] Alphabet argues that the legislator took a conscious choice to mandate that the pricing be based on

1199 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 3.

1200 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 175.

1201 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 175. Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 489, 492–497, and 509.

1202 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 4.

1203 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 518-520.

1204 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 524.

1205 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 528.

1206 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 509, and Alphabet's response to the Revised Measures, Doc ID […], paragraph 70.

1207 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 489, and Alphabet's response to the Revised Measures, Doc ID […], paragraph 70.

FRAND principles that necessarily exclude a cost-based approach, which can only be used if explicitly established by applicable legislation. [1208]

(998) Alphabet concedes that pricing differences may be appropriate depending on the eligible beneficiary, efficiency considerations, and transaction costs,[1209] and rejects that revenues from other business activities are relevant for assessing the FRAND nature of a pricing strategy.[1210] In this context, Alphabet argues that revenues obtained from providing ads services should not be taken into account to establish FRAND pricing terms for the purpose of Article 6(11) of Regulation (EU) 2022/1925, [1211] arguing that these compensate for an entirely different service. [1212]

(999) Alphabet maintains that using prices charged for a comparable service in a competitive market is the appropriate approach to establishing FRAND pricing.[1213] However, Alphabet itself acknowledges that "*given the novelty of the [article] 6(11) obligation there are no very obvious benchmarks*",[1214] and in this sense notes the lack of search datasets that offer the same level of dimension, scope and usability as the data to be shared under Article 6(11) of Regulation (EU) 2022/1925.[1215]

(1000) Alphabet also argues that the fact that Article 6(11) of Regulation EU 2022/1925 and recital 61 of that regulation do not provide further guidance as to what is to be considered FRAND access terms to these data, unlike Article 6(12) of Regulation EU 2022/1925 and its recital 62, which refer specifically to price benchmarks, is not decisive. In fact, Alphabet supports the use of price benchmarks in determining the FRAND pricing terms also in the context of Article 6(11) of Regulation EU 2022/1925.[1216]

(1001) Based on this interpretative framework, Alphabet claims to have conducted extensive research on possible value-based pricing approaches to validate its own approach, including:

(a) Revenue-based and incremental revenue-based approaches, where the price would be determined by applying a royalty percentage to the total or incremental revenue of the beneficiary. Incremental revenue would be determined in this context by removing a baseline amount (e.g., a given beneficiary's total revenue from the period prior to the data sharing) from total revenue.[1217]

(b) Volume-based and incremental volume-based approaches, where the price would be determined by multiplying the total EU query volume received by the OSE of a given beneficiary by a unit price (i.e. per thousand data points, also

---

1208 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 4; Alphabet's reply to RFI 3 of 25 February 2026, Doc ID […], paragraph 4; Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 489, 504 and 505.

1209 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 176.

1210 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 5; Alphabet's response to the Preliminary Findings, Doc ID 2420-2, paragraph 508.

1211 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 5.

1212 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 508.

1213 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 518 – 520, and 522.

1214 Annex to Alphabet's reply to RFI 5 of 6 September 2024, "Internal pricing assessment", Doc ID […], page 2.

1215 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 47, paragraphs 179 and 182; Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 9; Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 524.

1216 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 521.

1217 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 172.

referred to as "CPM"). Similarly to the incremental revenue-based approach above, incremental query volume would be determined in this context by removing a baseline volume (e.g., a given beneficiary's total EU query volume from the period prior to the data sharing).[1218]

(c) Pricing approach based on total size of the Search Data (i.e. unit price multiplied by the number of records included in the dataset) received by the beneficiary, irrespective of query volume realised by the beneficiaries' OSE. In this context, Alphabet used ComScore qSearch data,[1219] third-party Google SERP datasets,[1220] and search syndication offerings, including offers from Google, Bing and Brave search syndication APIs, as external reference points for pricing.[1221]

(1002) Alphabet also claims having considered a cost-based pricing approach, where the price would reflect Alphabet's internal costs of storing and providing the dataset, such as *inter alia* the costs of storage, and/or the costs of preparing and maintaining the dataset more broadly.[1222] In addition, Alphabet notes that if a cost-based pricing approach were to be used, the costs to be considered should include, in addition to those incremental for the provision of access to Search Data, those related to all cost of running and maintaining the Google Search's infrastructure.[1223]

(1003) The application of the value-based approaches considered by Alphabet as outlined in recital (1001) above, based on the company's own internal analyses and estimates, would imply total costs that range widely, between USD [0-100,00] and USD [20-25] billion. More specifically, Alphabet's internal analysis leads to:[1224]

(a) the following maximum price estimates per beneficiary for a quarterly data set:

(1) USD [pricing estimate] million, under a (25%) incremental EU revenue share approach;

(2) USD [pricing estimate] – USD [pricing estimate] million, under a (2% - 3%) total EU revenue share approach;

(3) USD [pricing estimate] – USD [pricing estimate] million, under a (50%) share of incremental EU query volume approach, based on USD 1 – USD 10 CPM;

(4) USD [pricing estimate] – USD [pricing estimate] million, under a (total) EU query volume approach, based on USD 0.02 – 1 CPM.

1218 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 173.

1219 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 174. According to Alphabet, ComScore has a custom qSearch data product, which covers search queries, query count, paid result and paid impression count, but which does not cover organic search results. The implied ComScore price can be calculated per unique query or per query volume.

1220 Alphabet's reply to RFI 5 of 6 September 2024, question 46, Doc ID […], paragraph 174. According to Alphabet, used selected Google SERP datasets compiled by third parties as listed with a publicly available pricing option on datarade.ai. The Google SERP offering on datarade.ai consists of SERP datasets and keyword datasets, as well as API services.

1221 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 174.

1222 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], question 46, paragraph 175. However, Alphabet notes in this respect that FRAND principles do not mandate such an approach and that a firm subject to FRAND pricing obligations is entitled to charge for the value that it delivers.

1223 Alphabet's response to the Revised Measures, Doc ID […], paragraphs 71-75.

1224 Annex to Alphabet's reply to RFI 5 of 6 September 2024, "Internal pricing assessment", DMA.100191ID0000234_GOOGLE-DMA6(11)-USPriv-00000163, Doc ID […], page 17.

(b) price estimates based on the total size of the quarterly 6(11) dataset ranging between USD [pricing estimate] million (based on USD 1 CPM) and USD [pricing estimate] billion (based on ComScore price per query).

(1004) In contrast, Alphabet itself estimates that under a cost-based approach the pricing would amount to USD [pricing estimate] (decreasing with the number of beneficiaries).[1225] This indicates that most of the estimated prices obtained following the revenue-based and volume-based approaches, considered by Alphabet, would be multiple times higher than the price under the cost-based approach. Only a few lower bound estimates would be within the same order of magnitude as the cost-based approach.

(1005) Upon examination of the various pricing approaches, including a cost-based one, even though Alphabet subsequently concluded that the latter is not FRAND,[1226] and considering that using a value based approach grounded directly on eligible beneficiaries' revenues or on query volume of their OSE would be too onerous to implement,[1227] Alphabet settled its benchmarking strategy on the value-based approach based on a benchmark unit price to be applied to the size of the dataset shared.[1228] The unit price of this method takes into account three market benchmarks (i.e., dataset reference points, as described under recital (1001)(c)).[1229]

(1006) Based on this method, Alphabet currently offers a tiered pricing model, charging a fixed fee per 1 000 unique queries shared with eligible beneficiaries. These fixed prices vary depending on the EEA search revenue made in the preceding year by the respective eligible beneficiaries.[1230] Accordingly, eligible beneficiaries which made search revenue of less than EUR 500 million must pay EUR 3 per 1 000 unique queries access ("per unit"). Those with search revenue figures between EUR 500 million and EUR 1 billion must pay EUR 6 per unit. Eligible beneficiaries with search revenues above EUR 1 billion must pay EUR 9 per unit. In August 2024, Alphabet introduced an additional pricing tier for eligible beneficiaries with EEA search revenues below EUR 50 million, charging EUR 1.5 per unit.[1231]

(1007) Alphabet offers the possibility to request accessing data on a country-by-country basis (within the EEA). It is also possible to access portions of the dataset (e.g., 10% or 50%) at the same per unit rates.[1232] In addition, in August 2024 Alphabet introduced the option to purchase a one-time 5% sample dataset, before deciding whether to purchase a full dataset.[1233]

(1008) Under Alphabet's current offering, the indicative price for 10% of the full EEA dataset for a firm with an EEA search revenue of less than EUR 500 million would be approximately EUR 300 000, whilst acquiring the full 100% dataset would cost

---

1225 This upper bound price reflects the price paid under the assumption that there would only be a single beneficiary. The price would lower with each incremental beneficiary, as all fixed cost components would be divided across the number of beneficiaries.

1226 Alphabet's presentation of 12 February 2026, "The price for Google's search data is FRAND", Doc ID […], slide 4; Alphabet's reply to RFI 3 of 25 February 2026, Doc ID […], paragraph 4; Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 489, 504 and 505.

1227 Alphabet's presentation of 12 February 2026, Doc ID […], "The price for Google's search data is FRAND", slide 12.

1228 Alphabet's reply to RFI 5 of 6 September 2024, Doc ID […], questions 46 and 47, paragraphs 176 and 181.

1229 Alphabet Compliance Report, Google Search Chapter, paragraphs 109 and 110.

1230 Alphabet Compliance Report, Google Search Chapter, paragraphs 110 and 115.

1231 Alphabet Compliance Report, Google Search Chapter, paragraph 110.

1232 Alphabet Compliance Report, Google Search Chapter, paragraph 111.

1233 Alphabet Compliance Report, Google Search Chapter, paragraph 116.

around EUR 3.3 million. For a large firm with an EEA search revenue exceeding EUR 1 billion, the costs would be around EUR 1.0 million for 10% of the dataset and EUR 9.9 million for the full 100% dataset.[1234]

(1009) In its response to the Preliminary Findings, Alphabet claims that the proposed pricing specifications are convoluted and unworkable in practice due to the complex calculations relating to the incremental costs incurred, the common costs allocation across an unstable number of recipients, and the system of exceptions envisaged for different categories of recipients. [1235]

(1010) Furthermore, Alphabet argues that capping the returns at the group-level weighted average cost of capital ("WACC") is not appropriate, as it reflects Alphabet's credit risk and does not capture the specific incremental risks and capital employed for complying with Article 6(11) of Regulation (EU) 2022/1925. Alphabet claims that it further penalizes Alphabet for being a good creditor.[1236]

(1011) Alphabet also claims that respondents to the public consultation broadly criticize the Commission's alleged focus on costs instead of value and that the only respondents in support of the cost-based approach were the potentially eligible beneficiaries. [1237]

4.5.1.2. The views of market participants

(1012) Market participants have also provided their views on FRAND compensation in the context of Article 6(11) of Regulation (EU) 2022/1925, on Alphabet's current offering, and on the Commission's preliminary measures through the public consultation opened on 28 April 2026.

(1013) [Market participants] claim that the prices under Alphabet's current offering are disproportionate and too expensive, making them unaffordable for many third-party search engines.[1238]

(1014) All market participants have considered a cost-based approach to be a conceivable approach for FRAND compensation, with most market participants advocating it as being the most appropriate approach in the context at hand. [1239] This view is aligned with that of a substantive group of respondents to the public consultation.[1240] Only a minority supported a fundamentally different approach. [1241]

1234 Annex Q2.02 to Alphabet's reply to RFI 3 of 25 February 2026, Doc ID […].

1235 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 531-534.

1236 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 531-532.

1237 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 498-500.

1238 See Legal Opinion on Search Data Access under Article 6(11) DMA of 4 June 2024 submitted by [market participants], Doc ID […], page 7.

1239 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5, paragraph 1.3; [market participant]'s reply to RFI 3 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], question 25; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5.

1240 Aside from market participants that are potential beneficiaries, this perspective is also reflected in submissions from [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], and a number of private citizens.

1241 For instance, [third party], [third party], [third party], argue that a purely incremental cost-based approach risks turning the remedy into a subsidy for competitors and consider that the pricing methodology should reflect investments in data collection.

(1015) In this context, market participants and a substantive group of respondents to the public consultation emphasised that since the objective of Article 6(11) of Regulation (EU) 2022/1925 is to enable contestability, the approach specified should prevent the gatekeeper from further benefitting from its strong market position.[1242] In view of this objective, they considered that a cost-based approach limited to the costs of providing the data would be the most appropriate to establish a pricing that can be considered FRAND.[1243]

(1016) Furthermore, the costs of providing the data are generally viewed as being limited in scope (e.g., Alphabet's reasonable costs of collecting, processing, anonymizing, and providing the data, plus a fair return on any innovation that adds demonstrable value to the dataset) and are expected to be low.[1244] A value-based approach is seen as being prone to incorporating a hold-up value and risking undermining the pro-competitive purpose of the provision.[1245] The data is further viewed to be generated as a by-product of user interactions and as not embodying autonomous economic value.[1246] Another market participant argues that FRAND pricing terms for the Search Data should approximate the terms that would exist in a competitive environment, where multiple search providers possess comparable human-interaction datasets and offer such data to customers on competitive terms. In such an environment, the market participant claims that competition would drive pricing towards the cost of collecting, processing, and providing the data.[1247]

(1017) Market participants further argue that a cost-based approach is supported by the US Google Search proceedings, where the court ordered Alphabet to make search data available at marginal cost, as well as by its use in the telecommunications sectors, where similar situations of power asymmetries commonly arise.[1248]

(1018) The majority of market participants further consider that the compensation should not feature any margin, since most of them argue that it would undermine the FRAND requirement by allowing gatekeepers to make profits out of a legal obligation to provide access to data. In particular, [market participants] oppose any margin, with [market participant] arguing that it would reintroduce rent components and undermine the FRAND requirement. [Market participants] propose that gatekeepers should provide the data for free, among other reasons because of their non-compliance with the DMA deadline. [Market participant] questions the need for a margin, suggesting that it would allow Alphabet to earn a profit on the provision of data that it is required to make available under Article 6(11). [Market participant]

1242 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 1, paragraph 1.3; [market participant]'s reply to RFI 3 of 16 January 2026, Question 1, Doc ID […].

1243 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; a market participant's reply to RFI PO 1 of 9 March 2026, Doc ID […], question 25; and responses to the public consultation from [respondents to the public consultation].

1244 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], question 25.

1245 See a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], question 25.

1246 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5.

1247 See a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], question 25.

1248 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], questions 1 and 5.

considers that no margin is justified, as marginal cost accurately reflects the direct and objectively verifiable costs of providing access to the data, and allowing Alphabet to receive further benefits would be contrary to the objective of Article 6(11) of Regulation (EU) 2022/1925.[1249] This view is confirmed by other respondents to the public consultation.[1250]

(1019) Some market participants would consider some narrowly circumscribed margin justified. [Market participant] believes that any pricing above cost recovery should be treated carefully, and that a limited and minimal margin may be acceptable if it reflects clearly identified, incremental risks of providing access, but only if it is transparent, pre-defined, and subject to regulatory oversight. [Market participant] considers that a limited margin may be appropriate to reflect commercial risk and capital costs, as long as it is transparent. Another market participant considers that a premium over cost would only be justified to the extent that the data adds genuine incremental value attributable to that provider's own innovation and investment over competing alternatives.[1251]

(1020) Overall, market participants' feedback suggests that Alphabet's proposal is too onerous and not considered to be a FRAND-compliant solution. Market participants overall express concerns over value-based approaches, such as the one currently followed by Alphabet, and advocate instead for a cost-based approach with no or limited margin.

4.5.2. Measures

(1021) The Commission considers that, to meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must provide the Search Data to eligible beneficiaries against a compensation that strictly reflects the incremental costs incurred by Alphabet for the purpose of making such Search Data available plus a reasonable return, corresponding to a return on the capital employed for that purpose that must not exceed Alphabet's WACC.

(1022) By way of exception to recital (1021), Alphabet should not be constrained to a compensation strictly reflecting incremental costs incurred for the purpose of making such Search Data available and a reasonable return corresponding to a return on the capital employed for the purpose of the provision of access to Search Data that must not exceed Alphabet's WACC in the event that (i) Alphabet demonstrates that it would not be able to cover the costs efficiently incurred to collect the relevant data, including a reasonable return, from its own commercial use of that data,[1252] or (ii)

1249 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 7, RFI 2 of 16 January 2026, Doc ID […], question 7; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 7; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 7; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 7, [market participant]'s reply to RFI 3 of 16 January 2026, Doc ID […], question 7; [market participant]'s reply to RFI 2 of 16 January 20216, Doc ID […], question 1.

1250 For example, [respondent to the public consultation]argues that a WACC uplift is unnecessary because the relevant capital investment is already in place and WACC estimation can itself be contested; [respondent to the public consultation]also takes the view that pricing should not include capital return.

1251 See a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], question 25.

1252 The revenue from Alphabet's commercial use of the data should at least include Google Search revenue, which is defined in this context as any revenue directly or indirectly attributable to the provision, operation, or monetisation of the Google Search service, including revenues generated through search advertising, intermediation of search-related traffic, and any other commercial activities deriving value from search queries or search-related user interactions.

when an eligible beneficiary operates at a very large scale.[1253] In these circumstances, Alphabet may also be entitled to a margin which cannot exceed the operating margin, in percentage terms, of Alphabet's Google Search business, and provided that any resulting terms, taking into account the relevant circumstances, remain FRAND within the meaning of Article 6(11) of Regulation (EU) 2022/1925 as outlined in section 4.5.3.1. [1254]

(1023) Notwithstanding recital (1022), micro, small and medium-sized enterprises (SMEs), as defined by Article 2 of the Annex to Commission Recommendation 2003/361/EC,[1255] must be exempted from paying more than the incremental costs incurred by Alphabet for the purpose of making Search Data available and a reasonable return on the capital employed for that purpose that must not exceed Alphabet's WACC, irrespective of whether Alphabet demonstrates its inability to cover the efficiently incurred costs as set out under recital (1021), above.

(1024) Whether Alphabet negotiates the compensation with certain eligible beneficiaries in line with recital (1034) is without prejudice to the application of the cost-based calculation methodology, in line with recital (1021), and cost-allocation principles for all other eligible beneficiaries. In particular, the fact that Alphabet negotiates the compensation with certain eligible beneficiaries in line with recital (1034) must not affect the cost base or the pro rata allocation parameters applicable to other eligible beneficiaries, which must be calculated as if all eligible beneficiaries were subject to the cost-based methodology, specifying a compensation which reflects the incremental cost incurred for the provision of access to Search Data and a reasonable return on the capital employed for that purpose.

(1025) Cost items that qualify as strictly incremental and incurred by Alphabet for the purpose of making the Search Data available to eligible beneficiaries include all costs (irrespective of whether they could be otherwise categorised as fixed or variable costs) pertaining to the following activities: [1256]

(a) Preparing and formatting the Search Data with a view to making the dataset available. This includes all costs directly attributable to the data-sharing-specific further processing of data already stored in Alphabet's databases, that would not be incurred in the absence of the data-sharing provision, including any data-format adaptations, sub-setting or transformations performed with the objective of protecting data subjects, such as anonymisation.

(b) Storage, that is, storage costs linked to making the Search Data available to eligible beneficiaries. Storage costs should only be part of the cost calculation to the extent that the storage environment is used for storing data with a view to making it available to eligible beneficiaries.

1253 Very large scale is being defined in this context as having more than 45 million monthly active end users established or located in the Union and an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years, or an average market capitalisation or equivalent fair market value amounted to at least EUR 75 billion in the last financial year, calculated in line with Articles 3(2)(a) and (b) of Regulation (EU) 2022/1925.

1254 This means that the resulting pricing terms should allow the beneficiary to obtain effective access to the Search Dataset to be able to optimise its search services without Alphabet maintaining or obtaining an unfair advantage.

1255 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Official Journal L 124, 20/05/2003 PAGE 0036-0041.

1256 Including common costs arising from making the data available.

(c) Dissemination, that is, costs incurred in the process of electronically transmitting data to eligible beneficiaries, including technical onboarding costs and the costs of operating the Search Data access tools.

(1026) The above incremental costs can be classified along two dimensions depending on (i) whether they are recurrent or one-off and (ii) whether they are beneficiary-specific or common across beneficiaries. This results in four categories of incremental costs: one-off beneficiary-specific costs, such as beneficiary-specific technical onboarding costs; one-off common costs, such as the development and set-up of the data sharing service; recurrent beneficiary-specific costs, such as transmission costs attributable to a specific beneficiary; and recurrent common costs, such as overhead costs common across beneficiaries.

(1027) The reasonable return on the capital employed for the purpose of making the Search Data available, that Alphabet may also include as part of the compensation, must not exceed Alphabet's WACC. Capital employed for the purpose of making the Search Data available must be understood as the incremental capital strictly necessary for making the Search Data available.

(1028) Alphabet must implement a per-beneficiary payment scheme which contains a fixed and variable component (two-part tariff). The fixed component ("fixed fee") must be determined independently of the duration of access, the volume of data consumed and the timing at which the beneficiary obtains access. The fixed fee covers, in addition to one-off beneficiary-specific costs, a share of the one-off common costs, which must be allocated on the basis of the allocation key referred to in recital (1031)(a). Alphabet must offer beneficiaries the possibility to pay their fixed fee over the duration of the contract, without prejudice to Alphabet's right to obtain full payment of the fixed fee should a beneficiary decide to discontinue its access to the Search Data before the last invoicing period.[1257] The variable component covers the beneficiary-specific recurrent costs of making the data available in a given year, as well as the recurring common costs during that year, which must be allocated on the basis of the allocation key referred to in recital (1031)(c).[1258]

(1029) Only incremental costs that are clearly attributable to making the Search Data available may qualify for the purpose of determining the compensation. Costs must not qualify merely because they arise in connection with the obligation. Alphabet must be able to demonstrate that all incremental cost items are objective, measurable, verifiable and proportionate to the purpose of making the data available. Overhead, sunk costs, investments in data collection, processing and storage not attributable to making the Search Data available, speculative risks, ordinary business and general compliance expenses, or dispute-related legal costs do not qualify for inclusion in the cost base to identify the incremental cost incurred by Alphabet in the process of making the Search Data available to eligible beneficiaries.

(1030) Incremental costs related to the development, set-up and scaling of the data sharing mechanism, shall be considered as capital employed for the purpose of making the Search Data available to the extent that they reflect expenditures for the development of assets, systems or capabilities that are expected to be used over multiple years.

(1031) One-off and recurrent incremental cost items that are common to different beneficiaries must be allocated in a reasonable, transparent and predictable manner,

---

1257 No return on capital must be due after a beneficiary has paid the fixed fee.

1258 For the purposes of calculating the fee Alphabet may charge for accessing the data samples B and C, as referenced in sections 4.6.3.2.2 and 4.6.3.2.3, Alphabet should only take into account recurring beneficiary-specific costs.

having regard to the nature of the relevant cost item and the point in time at which it is incurred. The volume of access requests cannot be known in advance and may vary over time. The allocation methodology must not result in unjustified differences in treatment between beneficiaries obtaining access at different points in time. To this effect, Alphabet must:

(a) determine the initial per-beneficiary share of the one-off costs based on a reasonable and justified estimate of the expected number of beneficiaries at the time the access mechanism is first made available, as determined following the process described in section 4.6.6.2, with those costs to be shared equally among all such expected beneficiaries;

(b) apply the same fixed component, as described under recital (1028) and established following the methodology laid out in point (a), to all actual beneficiaries irrespective of the time they start having access, subject only to differences objectively justified by beneficiary-specific one-off costs;[1259]

(c) recurrent common costs must be shared equally among the beneficiaries receiving access during a given year.

(1032) In line with section 4.6.6.2, upon request, Alphabet must provide information setting out the basis for the calculation of the compensation in sufficient detail so that eligible beneficiaries are able to assess whether the above-stated requirements are met. Alphabet must maintain, for each year, information supporting the calculation of the compensation and, upon request of the beneficiaries, provide them with a non-confidential version thereof, at the appropriate level of granularity to ensure both a sufficient degree of transparency as well as the protection of confidential information. Confidential and non-confidential versions of the information setting out the basis for the calculation of the compensation must also be provided to the Commission.

(1033) Alphabet must attempt to resolve any disagreement on the application of the above-specified calculation methodology directly with beneficiaries in good faith. Should a disagreement on any elements of the compensation persist, Alphabet must not prevent beneficiaries from raising such disagreement with the Commission. The Commission reserves the right to take action in accordance with its powers under Regulation (EU) 2022/1925 to verify Alphabet's compliance with the above terms, including auditing Alphabet's costs to ensure they are reasonable and proportionate to the claimed expenses. This provision is without prejudice to the beneficiaries' right to initiate legal proceedings before the competent courts.

(1034) Regarding eligible beneficiaries that are also designated gatekeepers under Article 3(4) Regulation (EU) 2022/1925 in relation to an online search engine core platform service, Alphabet may deviate from the FRAND compensation specified in this Decision. In that case, Alphabet must still negotiate, in good faith, and within the limits set out in Article 6(11) of Regulation (EU) 2022/1925, the applicable compensation provided that any resulting terms, considering the relevant circumstances and position of the two parties, remain FRAND within the meaning of Article 6(11) of Regulation (EU) 2022/1925 and otherwise comply with that provision.

[1259] For instance, where additional eligible beneficiaries obtain access after the initial intake period, those beneficiaries shall be subject to the same fixed component corresponding to one-off common costs as beneficiaries that obtained access earlier, subject only to adjustments reflecting objectively justified beneficiary-specific one-off costs.

4.5.3. The Commission's assessment

4.5.3.1. FRAND under Article 6(11) of Regulation (EU) 2022/1925

(1035) Article 6(11) of Regulation EU 2022/1925 mandates gatekeepers to provide third-party undertakings providing online search engines with access to ranking, query, click and view data generated by end users on FRAND terms. In application of this provision, Alphabet is allowed to establish pricing terms governing the provision of access to Search Data to eligible beneficiaries, as long as these pricing terms are FRAND.

(1036) Article 6(11) of Regulation EU 2022/1925 does not provide further guidance as to what is to be considered FRAND access terms to these data, nor does accompanying recital 61 of Regulation EU 2022/1925. Within the same regulation, the legislature also relied on the FRAND condition in its Article 6(12) of Regulation EU 2022/1925, which is further explained in recital 62 of that regulation. That provision, which aims to ensure that gatekeepers do not apply different conditions of access to gatekeeper services to business users, requires that general access conditions imposed on business users of software application stores, online search engines, and online social networking services be FRAND. In that case, the EU legislature explicitly contemplated a number of price benchmarks to assess the fairness of general conditions or prices imposed for accessing these core platform services.[1260] These price benchmarks relate to a number of comparable situations where access to the same or a similar service may already be provided against remuneration.

(1037) However, online search engine operators, including gatekeepers themselves, do not provide access to ranking, query, click and view data at all. Therefore, in the Commission's view, there are no comparable situations where a market price is charged to give access to the data covered by Article 6(11) of Regulation EU 2022/1925 or to provide a similar service. As Alphabet itself recognises,[1261] there are no comparable market offerings readily available to contemplate the possibility of finding a benchmark that can be operational for determining the FRAND pricing of the Search Data.

(1038) Moreover, the Commission's legislative proposal[1262] did not refer to pricing benchmarks in order to define FRAND terms in relation to what ultimately became Article 6(11) of Regulation EU 2022/1925 and recital 61 thereof[1263] and, in any event, the EU legislature did not refer to pricing benchmarks (or other benchmarks) to that effect in the context of Article 6(11) of Regulation EU 2022/1925 and recital 61, as finally adopted.[1264]

1260 Recital 62 of Regulation EU 2022/1925 outlines that "[t]he following benchmarks can serve as a yardstick to determine the fairness of general access conditions: prices charged or conditions imposed for the same or similar services by other providers of software application stores; prices charged or conditions imposed by the provider of the software application store for different related or similar services or to different types of end users; prices charged or conditions imposed by the provider of the software application store for the same service in different geographic regions; prices charged or conditions imposed by the provider of the software application store for the same service the gatekeeper provides to itself."

1261 Annex to Alphabet's reply to RFI 5 of 6 September 2024, "Internal pricing assessment", Doc ID […], page 2.

1262 See Commission Proposal for a Regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act) of 15 December 2020, COM/2020/842, recital 56.

1263 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 497.

1264 Moreover, contrary to Alphabet's view, the fact that the EU legislature used the term FRAND, rather than expressly prescribing cost-based pricing, cannot be construed as meaning that a value-based

(1039) In the absence of specific guidance relating to the concept of FRAND in the context of Article 6(11) of Regulation EU 2022/1925, in order to make that concept operational, it is appropriate to examine the objectives of that provision and to consider the relevant economic and regulatory circumstances of the specification.[1265] This means that the objectives of Article 6(11) of Regulation EU 2022/1925, as well as the broader goals of fairness and contestability that justify regulatory action through Regulation EU 2022/1925,[1266] should be taken into account to understand the scope of the FRAND obligation when it comes to pricing measures governing eligible beneficiaries' access to Search Data.

(1040) Article 6(11) of Regulation EU 2022/1925 and the accompanying recital 61 of the same regulation, clarify that the value of online search engines increases with the number of their users, because they benefit from information derived from users' interaction with the online search engine. In this context, the value of Alphabet's Search Data stems from these users' behavioural signals. Since gatekeepers providing online search engines like Alphabet have a privileged access to these data, which constitutes an important barrier to entry and expansion, Article 6(11) of Regulation EU 2022/1925 strives to achieve a more balanced situation in which eligible beneficiaries may be put in a position to contest Google Search by optimising their services through the use of Search Data. Accordingly, to ensure that the objectives of Article 6(11) of Regulation EU 2022/1925 are effectively achieved, FRAND pricing terms for accessing Search Data should ensure that such access is not unduly restricted or limited.

(1041) Furthermore, considering the broader goals enshrined in Regulation EU 2022/1925 of ensuring contestability in EU digital markets, the FRAND nature of the pricing terms on which eligible beneficiaries may access Search Data should ensure that such access is not only possible, but that it is provided in a way that is conducive to these goals. In this sense, when specifying Alphabet's FRAND pricing terms under Article 6(11) of Regulation EU 2022/1925, the following considerations should be taken into account.

(1042) Given the large difference in scale and access to key user interaction data, eligible beneficiaries are in a disadvantaged position with respect to Alphabet. In addition, other than the FRAND price to be paid to Alphabet, accessing Search Data for them also means facing considerable costs for the onboarding of these data (such as investments in an adequate infrastructure for the integration of the new data, or in ensuring that they comply with the safety features required).[1267] Finally, since the

---

methodology was intended. See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 504.

1265 See for instance Judgment of 16 July 2015, Huawei Technologies Co. Ltd v ZTE Corpage and ZTE Deutschland GmbH, C-170/13, EU:C:2015:477, paragraphs 54-56, where the court recognised that, when assessing what is required by FRAND terms, "*due account must be taken of the specific legal and factual circumstances in the case*". The Court also referenced its judgment in Post Danmark, C-209/10, EU:C:2012:172, paragraph 26 and the case-law cited, where it noted that "*[i]n order to determine whether a dominant undertaking has abused its dominant position by its pricing practices it is necessary to consider all the circumstances and to examine whether those practices tend to remove or restrict the buyer's freedom as regards choice of sources of supply, to bar competitors from access to the market, to apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage, or to strengthen the dominant position by distorting competition.*"

1266 Article 1(1) of Regulation (EU) 2022/1925.

1267 See [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], Question 6; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], Question 6; [market participant]'s reply to

actual benefit of the Search Data accessed is an indirect one that derives from the improvement of their services, eligible beneficiaries will at first be making an upfront investment with uncertain returns. [1268]

(1043) In addition, in light of the broader DMA goal of ensuring fairness in digital markets in general and in the market for online search engines in particular, and as foreseen in Article 8(8) of Regulation EU 2022/1925, while not impairing Google Search's incentives to continue providing its own search services, pricing terms for accessing Search Data must neither give rise nor maintain disproportionate advantages for Alphabet. In this sense, when specifying Alphabet's pricing measures, it should be considered that Search Data are essentially generated as a result of users' behaviour in Google Search. Thus, Search Data are a necessary by-product of Alphabet's provision of online search services. Therefore, Alphabet already monetises the collection of the Search Data, regardless of their further sharing with eligible beneficiaries.

(1044) Finally, the Commission wishes to recall that FRAND principles often seek to balance the interests of the entity giving access to the relevant resources, which is normally in a superior bargaining position, and those of the access seekers which tend to be in less advantageous positions. As such, FRAND principles have been used in various areas, including in negotiations for accessing standard essential patents, including in the application of EU competition law,[1269] and in the field of electronic communications.[1270] In this sense, as further developed in section 4.5.3.2, the use of FRAND in other regulatory contexts where there is also a need to ensure access for all entitled beneficiaries to a critical resource, which is usually held by a single entity, may be relied upon to inform the specified pricing terms under Article 6(11) of Regulation EU 2022/1925.[1271]

(1045) Against this background, the Commission is of the view that the FRAND pricing terms on which Alphabet must provide access to Search Data to eligible beneficiaries should allow those beneficiaries to obtain effective access to such data to be able to optimise their search services without maintaining or providing this gatekeeper with an unfair advantage.

RFI 3 of 16 January 2026, Doc ID […], Question 6; [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], question 6, paragraph 6.5.

1268 See for instance the response from [market participant] to question 3 and 4 of RFI 3 of 16 January 2026, Doc ID […], where the company explains that improvements to its search offering will not be immediate. See also [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], paragraph 6.5.

1269 Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements, C/2023/4752, OJ C 259, 21.7.2023, and Guidelines on State aid for broadband networks, C/2022/9343, OJ C 36, 31.1.2023.

1270 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018, and Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act), OJ L, 2024/1309, 8.5.2024

1271 Yann Méniére (2015), Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms – Research Analysis of a Controversial Concept, JRC report, Doc ID […], page 17.

4.5.3.2. Justifying a cost-based approach to FRAND pricing measures under Article 6(11) of Regulation (EU) 2022/1925

(1046) As Alphabet acknowledges, in general, undertakings should be compensated for the provision of key inputs to their customers.[1272] However, compensation for granting such access, including when the law mandates it to take place under FRAND terms, may be calculated on the basis of various approaches, including value-based or cost-based ones. While these approaches differ in their respective starting points, both allow to calculate the compensation that may be requested in exchange for the input that a given undertaking provides. Under a cost-based approach, the calculation starts from the costs incurred by the access provider in making a given input available, potentially with an additional margin. Under a value-based approach, the calculation seeks to establish the economic value of the input by reference to market-based indicators, typically comparable market transactions.

(1047) Against this background, the Commission is of the view that Alphabet's compensation for the Search Data shared in the form of specified FRAND pricing measures under Article 6(11) of Regulation EU 2022/1925 should follow a cost-based approach for the following reasons.

(1048) *First*, the determination of FRAND pricing is not a single, universal concept and often depends on the circumstances and the specific context. The EU legislator has prescribed the FRAND nature of conditions, including pricing, on previous occasions without prescribing a uniform methodology across contexts. [1273] As explained in recital (1039), it is therefore necessary to interpret the FRAND requirement in light of the objectives and specific context of Article 6(11) of Regulation EU 2022/1925. Alphabet's claim that the case law and industry practice uniformly point to a value-based approach to FRAND pricing based on market-based benchmarks is incorrect.[1274] At most, the materials relied on by Alphabet show that FRAND pricing *may* take value into account in certain contexts.[1275] They do not establish that FRAND pricing requires a value-based approach, let alone that Alphabet must be allowed to capture the value that beneficiaries may derive from access to the data.

1272 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 503.

1273 See, for instance, Article 15(1) of the Audiovisual Media Services Directive, OJ L 95, 15.4.2010, where it is stipulated that FRAND conditions should govern broadcasters' access to certain television broadcasting rights, but where a concrete pricing approach is not determined, or Section 5.2.4.4 of the Guidelines on State aid for broadband networks, C/2022/9343, OJ C 36, 31.1.2023, where three different approaches to setting FRAND prices for the wholesale access products are offered.

1274 See recital (996).

1275 See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 493–497, referring to Judgment of 27 June 2012, *Microsoft v Commission*, Case T-167/08, ECLI:EU:T:2012:323; Commission Decision of 13 December 2011, *IBM Maintenance Services*, Case COMP/AT.39692; Commission Decision of 14 July 2010, *British Airways/American Airlines/Iberia*, Case COMP/AT.39596; Commission Decision of 23 May 2013, *Continental/United/Lufthansa/Air Canada*, Case COMP/AT.39595; Commission Decision of 23 July 2004, *Scandlines Sverige AB v Port of Helsingborg*, Case COMP/A.36.568/D3; Judgment of 14 February 1978, *United Brands v Commission*, Case 27/76, ECLI:EU:C:1978:22; Judgment of 6 April 1995, *RTE and ITP v Commission (Magill)*, Joined Cases C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98; Judgment of 14 September 2017, *AKKA/LAA*, Case C-177/16, ECLI:EU:C:2017:689; Judgment of 25 November 2020, *SABAM*, Case C-372/19, ECLI:EU:C:2020:959; Judgment of 10 July 2025, *DADA Music and UPFR*, Case C-37/24, ECLI:EU:C:2025:551; Judgment of 18 December 2025, *OSA*, Case C-161/24, ECLI:EU:C:2025:985; Commission Decision of 23 April 2025, *Apple – Online Intermediation Services – App Stores – Article 5(4)*, Case DMA.100109; *Microsoft Corp. v Motorola, Inc.*, No C10-1823JLR, 2013 WL 2111217; and *Ericsson, Inc. v D-Link Systems, Inc.*, 773 F.3d 1201.

(1049) In fact, neither of the case law nor the decisions Alphabet relied on state that a cost-based approach is inappropriate, or that FRAND pricing must universally be determined by reference to value. Several do not concern value-based pricing in a FRAND context at all,[1276] while others, including *United Brands* and *Scandlines Sverige*, in fact support a cost-based reasoning.[1277] This further shows that Alphabet's claim that cost-based approaches are used only when explicitly mandated by the applicable legislation is incorrect. [1278]

(1050) Alphabet's reliance on the idea that a FRAND price must reflect the intrinsic value is also misplaced. [1279] The cases relied on by Alphabet for that proposition concern abusive refusal to supply and excessive pricing contexts, where the concept of intrinsic value serves to distinguish value attributable to the product or service itself from the strategic value linked to market power or other types of leverage. [1280] It is not used to establish that value-based pricing must be preferred over a cost-based methodology.

(1051) *Second,* in specifying FRAND access pricing under Article 6(11) of Regulation EU 2022/1925, it is appropriate to also draw on relevant comparable contexts. In this respect, Alphabet's claim that the SEP valuation context constitutes the most relevant comparator is inaccurate. [1281] SEP licensing typically refers to agreements under which patent holders license standard-essential technology to manufacturers in exchange for royalties. In these cases, the remuneration is for the use of the patented technology, whose monetisation is secured through a time-limited exclusive right and takes the form of royalties paid by manufacturers that incorporate that technology into their own final products. That context differs materially from the subject matter of these proceedings, in which an incumbent-controlled input (Search Data) is required to be shared with beneficiaries. The value of such Search Data is largely derived from the fact that the input was accumulated over years under conditions of scale, entrenchment and self-reinforcing data advantages. Furthermore, Search Data are only used to optimise the search services of beneficiaries and therefore there is only an indirect link with the final product that the beneficiaries will offer to their users.

1276 Several invoked references under paragraph 494 of Alphabet's response to the Preliminary Findings, Doc ID [...], including *IBM Maintenance Services*, Case COMP/AT.39692, paragraph 72; *BA/AA/IB,* Case COMP/AT.39.596, paragraph 116; *Continental/United/Lufthansa/Air Canada,* COMP/AT.39.595, para. 148*;* or *Radio Telefis Eireann (RTE)* and *Independent Television Publications Ltd (ITP) v Commission*, joined Cases C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 91, as well as the references to the *travaux préparatoires* of the DMA do not discuss FRAND pricing at all, let alone the appropriate pricing methodology.

1277 *United Brands v Commission*, Case 27/76, ECLI:EU:C:1978:22, paragraphs 251, where the Court held that the excessiveness of a price could, inter alia, be determined by comparing the selling price with the cost of production, thereby disclosing the profit margin; *Scandlines Sverige AB v Port of Helsingborg*, Case COMP/A.36.568/D3, paragraphs 219–221 and 232–233, where the Commission expressly did not exclude assessing unfair pricing within a cost-plus framework, while rejecting the view that economic value could be determined mechanically by adding a pre-determined profit margin to costs.

1278 See recital (997).

1279 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 493.

1280 See for instance *Microsoft v Commission*, Case T-167/08, ECLI:EU:T:2012:323, paragraphs 138 and 141–142, on the distinction between intrinsic and strategic value, or *United Brands v Commission*, Case 27/76, ECLI:EU:C:1978:22, paragraph 250, on the charging of a price of a product deemed excessive for having no reasonable relation to its economic value, or *AKKA/LAA*, Case C-177/16, ECLI:EU:C:2017:689, paragraph 61, on the need for an undertaking holding a dominant position to show that its prices are fair by reference to objective factors.

1281 See recital (996).

(1052) Leaving aside the SEP context, which is not comparable as indicated above, EU regulatory frameworks governing the imposition of mandatory access terms and conditions, including pricing, show that, where access seekers are in an inferior bargaining position due to structural asymmetries, and effective competitive constraints are not sufficient to ensure fair and reasonable conditions, the regulated pricing may be cost-based.

(1053) For instance, in the first place, the European Electronic Communications Code (EECC)[1282] concerns access conditions to electronic infrastructure networks. It contains provisions allowing national regulatory authorities to impose access obligations[1283] on operators designated as having significant market power ("SMP"), which may thus be required to grant access to their infrastructure to other operators in the market on fair and reasonable terms, and may thus be required to offer *inter alia* cost-based pricing terms, to other operators in the market.[1284]

(1054) The Commission Recommendation on the regulatory promotion of gigabit connectivity further develops the methodological framework applicable in such cases. In particular, it indicates that cost-based pricing may be implemented by reference to a "long-run incremental cost plus" methodology, where wholesale access prices are based on the incremental costs of providing the access service plus a limited allocation of common costs and a reasonable return on capital.[1285] This approach comprises three core elements. First, it includes the long-run incremental costs of providing the wholesale access service. That is, the additional operating and capital costs that would not be incurred if the access service were not supplied. Second, it allows for allocation of common costs,[1286] which may be recovered through a structured margin. Third, it incorporates an appropriate return on capital invested, reflecting the cost of capital necessary to sustain efficient investments.[1287] Together, these elements ensure that access prices enable full recovery of efficiently incurred access-related costs, while preventing the inclusion of expenditures that are not causally linked to the provision of the regulated access service.

(1055) In the second place, the Data Act sets out rules governing fair, reasonable and non-discriminatory terms and conditions for the making available of data, including rules for the compensation of data holders.[1288] According to this framework, compensation for the data shared is based on a cost-based approach designed to prevent

---

1282 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018.

1283 In particular, Article 74 EECC provides that such cost-oriented pricing may be imposed where a market analysis identifies a lack of effective competition and risks of excessive pricing or price squeeze. This indicates that cost-based pricing may be relied upon as a corrective tool where pricing flexibility cannot be ensured. This supports the relevance of a cost-based approach in situations characterised by comparable structural imbalances.

1284 Chapter IV in conjunction with Annex IV of the European Electronic Communications Code. In particular, see Articles 61(3), Art. 79(2) and Art. 80(2) of the EECC.

1285 Commission Recommendation on the regulatory promotion of gigabit connectivity ("Gigabit Recommendation"), C/2024/0523 final, paragraphs 27 and following.

1286 Costs that are shared across multiple services but that are not directly attributable to a single service unit.

1287 Gigabit Recommendation, paragraphs 40, 43 and 44.

1288 Article 12(1) of the Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L, 2023/2854, 22.12.2023 ("Data Act"), provides that Chapter III applies "*where, in business-to-business relations, a data holder is obliged under Article 5 or under applicable Union law or national legislation adopted in accordance with Union law, to make data available to a data recipient.*" See also Article 1 (subject matter), Article 8 (FRAND terms) and Article 9 (compensation for making data available).

overcompensation of the data holder and ensure effective data access by stipulating (i) a narrowly defined set of data access-related costs, and (ii) the possibility of an additional margin in specific cases and depending on a number of factors.[1289]

(1056) On the cost side, only the costs necessary to make the data available can be taken into account under the Data Act.[1290] Incremental costs directly linked to putting in place and operating the access mechanism, such as preparing and formatting the dataset, selecting subsets, disseminating the data, including onboarding and verification of data recipients, storing it for the purpose of making it available, and any strictly necessary measures to protect certain data may be recovered, insofar as they are attributable to a specific data access request.[1291] In contrast, general overhead, sunk costs, speculative risks, ordinary business expenses and broad data cleaning or quality initiatives that are not necessary for a specific access request are explicitly excluded from the cost base.[1292]

(1057) What these frameworks indicate, for the present purposes, is that the access provider should be given a fair chance to recover the costs of making the input available without being allowed to derive undue advantages from the access obligation itself. In that way, a cost-based methodology helps to ensure that the access provider is not overcompensated and that pricing remains aligned with the objective of the obligation to make access effective for the benefit of the competitive process.

(1058) While cost-based approaches may in general lead to a lower pricing benchmark, in the present context, the use of a cost-based methodology is justified by the objective to facilitate entry and contestability in online search services and the need to enable beneficiaries to effectively optimise their search services, while ensuring that access providers, in this case Alphabet, have a fair opportunity to recover the costs of providing access to Search Data and receive a reasonable return on the capital employed for these purposes.[1293] However, as further explained in subsection 4.5.3.4, there may be specific circumstances in which Alphabet should not be constrained to price strictly on the basis of incremental costs, and in which a limited additional margin, or negotiations in good faith within the limits set out in Article 6(11) of Regulation (EU) 2022/1925, may be deemed appropriate.

(1059) *Third,* the choice of a cost-based approach is consistent with the views of all market participants inquired, who argue that a cost-based approach is necessary to prevent Alphabet from extracting excessive rents and to ensure fair and reasonable access to Google Search Data.[1294] In this respect, Alphabet's allegation that the Commission's assessment was shaped by leading questions or by the uncritical adoption of beneficiaries' views is unfounded. The Commission explicitly and neutrally solicited

---

1289 Recital 47 of the Data Act stipulates that, apart from the costs incurred in making the data available, the reasonable compensation may also include a margin depending on factors related to the data itself, such as volume, format or nature of the data.

1290 Data Act, Article 9(2)(a).

1291 Draft Guidelines for Reasonable Compensation under article 9 of the Data Act ("Draft Compensation Guidelines"), Doc ID […], Section 4.1, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/consultations/data-act-commission-seeks-feedback-draft-guidelines-reasonable-compensation

1292 Draft Compensation Guidelines, paragraph 34.

1293 See section 4.5.3.3. For the purpose of the determination of the pricing offer, costs related to the development, set-up and scaling of the data sharing mechanism should be considered as capital employed strictly for the purpose of making the Search Data available to the extent that they reflect expenditures for the development of assets, systems or capabilities that are expected to be used over more than one accounting period.

1294 See section 4.5.1.2.

input on different possible pricing approaches, including value-based ones.[1295] When the Commission invited market participants to assess whether a value-based approach based on a revenue-sharing mechanism [1296] could meet FRAND standards under Article 6(11), the large majority of respondents disagreed that this would be the case.

(1060) Moreover, many respondents to the public consultation, including those that do not operate an OSE and would therefore not directly benefit from a lower price, also regard the cost-based approach as a fair and contestability-enhancing approach.[1297]

(1061) *Fourth,* the Commission considers that the limited set of value-based pricing benchmarks identified by Alphabet in its analysis as indirectly relevant[1298] are inappropriate, for the reasons set out below, to establish a FRAND compensation for Search Data sharing under Article 6(11) of Regulation EU 2022/1925. In the specific circumstances of the present data sharing obligation, such a value-based approach is not suitable to constitute the main framework for determining FRAND compensation.

(1062) *In the first place,* the Commission considers that the use of value-based pricing benchmarks would necessarily require an exhaustive assessment of, at least, the underlying product and services exchanged, the bargaining position of the data provider and data buyers, the market characteristics, the context, and the type of investments required for providing the service. Alphabet has failed to substantiate the relevance of its proposed benchmarks through such an analysis.

(1063) The main value-based benchmarks put forward in this respect by Alphabet are syndication agreements, ComScore qSearch data and SERP datasets.[1299]

(1064) As regards syndication agreements, the Commission considers that these are not appropriate benchmarks. *Firstly*, search syndication is a direct input into a recipient's downstream search products. Search syndication allows a third-party online search engine to answer user queries instantaneously and with virtually no investment into online search technology. Its price therefore reflects the immediate monetisable value that the recipient attributes to this service. In the second place, it is also likely that existing search syndication agreements may not reflect competitive pricing dynamics, as would be required under FRAND terms, as they may embed an oligopolistic market premium, since the market for search syndication is extremely concentrated with mainly two providers, Microsoft and Alphabet itself.[1300] In

---

1295 See questions asked during public consultation, as well as questions asked and corresponding answers in [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], [market participant]'s reply to RFI 3 of 16 January 2026, Doc ID […], [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], a market participant's reply to RFI 1 PO of 9 March 2026, Doc ID […], [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], [market participant]'s reply to RFI 2 of 16 January 2026, Doc ID […], a market participant's reply to RFI PO 2 of 17 March 2026, Doc ID […] and [market participant]'s reply to RFI PO 3 of 17 March 2026, Doc ID […].

1296 For instance, royalties tied to incremental or total search revenue.

1297 Aside from potential beneficiaries, this perspective is also reflected in submissions from [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], [third party], and a number of private citizens.

1298 See Section 4.5.1.1.

1299 Alphabet's response to RFI 5 of 22 July 2024, Doc ID […], paragraph 174.

1300 CMA, Online Platforms and Digital Advertising market study, Final Report (2020) [online], paragraphs 3.7, 3.81, and 5.49, Available at:

contrast, access to Search Data under Article 6(11) of Regulation EU 2022/1925 concerns the provision of an intermediate input which, in combination with other inputs, may lead to improved independent online search services, which may thus be able to contest Google Search. Therefore, the incremental downstream commercial value and impact of the Search Data is indirect, and, at this stage, inherently uncertain and difficult to quantify. In the third place, the value of the data under syndication agreements is generated by individual query events, with each query having a direct and discrete value. In contrast, the Search Data derives its value from the aggregation of click and query interactions, with the comprehensive scope and diversity of the data enabling a deeper understanding of user behaviour and trends. Notably, the value distribution of the Search Data is more nuanced, with significant value concentrated in the "long tail" of less frequent queries, but most importantly deriving from the optimisation that can be performed by exploiting the overall breadth and diversity of the data, rather than from single queries. These fundamental differences in the nature, use and potential monetisation of the respective inputs makes syndication an unsuitable value-based pricing benchmark for pricing access under Article 6(11) of Regulation EU 2022/1925.

(1065) The same conclusion applies to SERP datasets. These datasets correspond to collections of structured data on online search engine results pages, offered by multiple providers with differing pricing models, data volumes, and coverage, which are commercialised on platforms such as "datarade.ai". These datasets typically lack search behavioural data.[1301] While it may be structurally closer to Search Data than syndication data, this data is not typically purchased for optimising online search services but is used to optimise advertising campaigns or to identify keyword trends for marketing purposes. Prices observed for such materially different uses therefore cannot be transposed directly and provide limited informative value for determining the appropriate remuneration.[1302] Moreover, to the extent that SERP datasets are generated by bots crawling the web, they do not contain information on search and clicking behaviour of real users. Therefore, they might be less informative for the purpose of optimising OSEs.

(1066) The custom ComScore qSearch data does not constitute a suitable value-based pricing benchmark either. In the first place, to the extent that such data is panel-based (i.e., based on a sample of users) or subject to other data generation processes, its generation entails significant investments. The Search Data in turn is passively generated, with less significant costs required from Alphabet to produce it.[1303] This fundamental divergence in cost structure further aggravates the lack of comparability between these potential benchmarks and the Search Data. A similar reasoning is

---

https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf (last accessed on 10 July 2026) (Doc ID […]).

1301 [third party] report "Desk Research on datarade.ai pricing schemes and B2B data sharing", Alphabet's response to RFI 4 of 22 July 2024, Annex A to RFI 4, Doc ID […].

1302 For example the "Google Search Results Data" (Doc ID 1894) available at https://datarade.ai/data-products/value-serp-api-google-search-results-data-traject-data (link last accessed on 10 July 2026) is offered for the following uses:
- *Inform organic SEO and content creation strategy.*
- *Track keyword rankings across millions of keywords.*
- *Identify industry trends and evolving Google SERPs.*
- *Blend with other data sources to identify revenue generating keywords.*
- *Optimize advertising campaigns based on evolving Google algorithms and search intent.*
- *Monitor local performance across geolocations.*
- *Track Google eCommerce performance.*

1303 See a market participant's reply to RFI PO 2 of 17 March 2026, Doc ID […], question 1.

applicable to data shared under syndication agreements. *Secondly*, to the extent that the custom ComScore qSearch data, including in customised or more granular forms, is designed to provide market intelligence to users,[1304] its price further reflects the value of such analytics, derived from the transformation of underlying data into actionable insights. Comscore qSearch data therefore targets fundamentally different customer audiences and serves fundamentally different purposes. Moreover, to the extent that the source of Clickstream datasets is a panel of internet users, any resulting dataset might not be reflective of search and clicking behaviour of the entire population, as it is contaminated by selection into the sample.

(1067) Given that, in view of the characteristics, scope and underlying monetisation mechanism of the data, the above-mentioned value-based pricing benchmarks relate to situations not comparable to the sharing of the Search Data in these specification proceedings, a simple transposition of the prices, as Alphabet proposes, would be inappropriate and would risk both overcompensating Alphabet and fail to achieve the objective of Article 6(11) of Regulation (EU) 2022/1925. Furthermore, Alphabet has not proposed any methodology for adjusting those benchmark prices to the specific circumstances of the sharing of the Search Data at issue.

(1068) The arguments put forward in Alphabet's response to the Preliminary Findings do not change this conclusion. Alphabet takes an overly simplistic approach, when it claims that the above-referenced benchmarks are relevant and should in fact be considered a floor to the price of the Search Data,[1305] due to their inferior volume and metrics and the fact that the Search Data allegedly allows to do much more than the benchmarks suggested by Alphabet. *Firstly*, that claim rests on the misconception that the Search Data can constitute a substitute for syndication data. Using the Search Data as a direct substitute for syndication, i.e. directly returning search results based on the mapping contained in the Search Data, is neither allowed[1306] nor practical, given the limited coverage, freshness and quality of the Search Data[1307] to be shared, as compared to the data available under search syndication.[1308] *Secondly*, as mentioned above,[1309] a properly conducted benchmarking exercise could not limit itself to a simplistic scaling of prices per query based on commercial datasets' pricing without any meaningful analysis of their comparability with the Search Data. Alphabet has failed to provide any analysis aimed at adjusting the proposed benchmarks to the specificities of the Search Data sharing. *Thirdly*, the fact that the investments associated with Alphabet's Search Data may be substantially higher than those underlying the proposed benchmarks confuses the nature of the relevant investment.[1310] The Search Data already exists and is generated and used as part of Alphabet's broader search operations, unlike the datasets specifically produced or commercialised for supply to third parties. It is not the result of an investment aimed at producing a dataset for access seekers, but the output of the wider ecosystem through which Alphabet's search engine operates accumulating user interactions and result-related signals along the way. Article 6(11) of Regulation (EU) 2022/1925 concerns the making available of the existing Search Data that Alphabet collects in the ordinary course of operations when running its own online search engine.

1304 [Market participants]'s response to RFI PO 3 of 17 March 2026, Doc ID […], question 1.

1305 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 524.

1306 See recital (824).

1307 See sections 4.3 and 4.4.4.1.

1308 Alphabet's claim that the pricing would distort the market for syndication data is therefore incorrect.

1309 See recital (1062) and following.

1310 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 525 and 528.

(1069) Taking into account the goal of Article 6(11) of Regulation (EU) 2022/1925, which is to open up the Alphabet's search data advantage to contestability, rather than pricing such advantage by reference to the value that it generates for Alphabet or that it could generate for beneficiaries, benchmarks that reflect the economic value of the data, whether for Alphabet or for beneficiaries of the Search Data, are not the appropriate reference point.

(1070) As such, rather than from market offerings that seek to capture the full commercial value of the underlying shared data, suitable benchmarks for pricing of the Search Data should be drawn from contexts involving access-enabling activities that are comparable to the one that Article 6(11) of Regulation (EU) 2022/1925 imposes on Alphabet. In this sense, and contrary to Alphabet's further arguments that the Commission failed to consider additional benchmark evidence, the Commission considered benchmarks referenced by market participants and Alphabet but discarded them, as they are not comparable to the access-seeking activity. The benchmarks are not suitable for third-party OSEs to optimise their search services and contest Google Search.

(1071) Alphabet's further arguments that when market-based benchmarking is not relied on, then the Commission should adopt an alternative pricing mechanism that factors in the investment savings of beneficiaries thanks to the use of Search Data, do not alter this conclusion either.[1311] In fact, for the reasons set out in recitals (1069) and (1070), and also in light of the scale, entrenchment and self-reinforcing data advantages through which the Search Data was accumulated by Alphabet over time, which is not comparable to that of the eligible beneficiaries, it would not be reasonable to treat any resulting investment savings for beneficiaries as a parameter for establishing Alphabet's compensation under Article 6(11) of Regulation (EU) 2022/1925.

(1072) *In the second place,* the Commission observes that the absence of suitable benchmarks was also an important consideration in the US courts' choice to pursue a cost-based approach, in the context of the remedies in *US v. Google*. The court noted that there was no evidence of a market for the Search Index data and that Alphabet had not provided an appropriate methodology to value it.[1312]

(1073) In view of the above, the Commission is of the view that a cost-based approach is appropriate to specify FRAND pricing measures in the context of Article 6(11) of Regulation (EU) 2022/1925.

4.5.3.3. Operationalizing Alphabet's cost-based pricing measures under Article 6(11) of Regulation (EU) 2022/1925

(1074) In view of the considerations set out in section 4.5.3.2, the Commission considers that it is appropriate to specify FRAND pricing measures for Alphabet in the context of Article 6(11) of Regulation (EU) 2022/1925 on the basis of a cost-based approach, in order to ensure that compensation gives Alphabet a reasonable opportunity to recover the costs incurred in the provision of access to Search Data, including a reasonable return on the capital employed for the provision of such access, although without creating or maintaining unfair advantages, as follows.

1311 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 527 and 528.

1312 See, US v. Google, memorandum opinion of 2 September 2025 page 147 et seq. (Doc ID […]) In the absence of a separate reasoning provided for the mandated sharing of user-side data, it appears reasonable to infer that the court's approach to compensation would not materially differ. User-side data is conceptually closer to the Search Data subject to the remedy.

(1075) In the case of Alphabet, the relevant incremental costs of providing access to the Search Data should be confined to those that are causally and directly linked to the provision of the Search Data to eligible beneficiaries, and should not include the general costs of operating Google Search and generating the underlying data, which are also incurred for the provision of Alphabet's own services and already recouped through its existing business model. In practice, as outlined in section 4.5.2, this would translate into the costs of preparing and formatting the data for sharing, the costs of storing the data for further dissemination, and the costs linked to disseminating it, plus a reasonable return on the capital employed for the purpose of making the data available, that must not exceed Alphabet's WACC.

(1076) Alphabet's claim that the costs to be considered should include, in addition to those incremental for the provision of access to Search Data, those related to the running and maintaining the infrastructure [1313], is not compatible with the non-rival nature of the Search Data, which remains available to Alphabet after their use by the eligible beneficiaries, without any decrease in its quantity or quality.

(1077) Alphabet also claims that the process for the allocation of common costs is ambiguous and leaves it with the risk of absorbing part of these costs in case of low demand. [1314] The Commission is of the view that the process it has laid out in 4.6.6.2 and recital (1031) is clear, transparent and predictable. The approach provides a fair chance to Alphabet to cover the incremental costs of providing access to the Search Data while not resulting in unjustified differences in treatment between beneficiaries obtaining access at different points in time. In fact, the process is already designed to minimize Alphabet's risk of stranded costs and, if total demand [1315] exceeds the number of initially expected beneficiaries, may even result in remuneration beyond strict cost recovery.[1316]

(1078) Furthermore, Alphabet claims that the Commission arbitrarily caps its return by relying on the group-level WACC, which is irrelevant for pricing, penalises Alphabet for its low credit risk, and fails to capture the incremental risks and capital employed for complying with Article 6(11) of Regulation (EU) 2022/1925. [1317] Contrary to these claims, allowing a reasonable return based on WACC does not constitute an arbitrary cap to Alphabet's pricing for the following reasons.

(1079) *First*, by allowing for a reasonable return on the capital employed on the provision of access to the Search Data the Commission takes into account that the capital invested for this purpose involves an opportunity cost. The WACC is the commonly accepted measure of the average rate of return that all providers of capital (debt and equity) require to provide financing to an undertaking and thus reflects such opportunity cost. As such, the WACC reflects not only the credit risk of a given undertaking, and consequently the return required by its creditors, but also the return that its equity investors require. In fact, in light of the historical WACC data provided by Alphabet, which reveals that [description of Alphabet's internal financials][1318]. Therefore, even if the latter is low, it has only very limited impact on the group WACC. [1319]

1313 Alphabet's response to the Revised Measures, Doc ID […], paragraph 75.

1314 Alphabet's response to the Revised Measures, Doc ID […], paragraph 74.

1315 Measured by the number of beneficiaries effectively obtaining access over time.

1316 See also in this respect section 4.6.6.2.3.

1317 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 532(e)

1318 Measured by the number of beneficiaries effectively obtaining access over time.

1319 Alphabet cost of debt is expected to be low in view of the company's very low debt burden and high proportion of equity, which is subordinate to debt and, thus, implies modest risk for debtholders.

(1080) *Second*, WACC is also typically used in the context of access price regulation, for instance, in the telecommunications sector. In applying price control obligations to operators with significant market power, national regulatory authorities (NRAs) use the WACC for determining the reasonable rate of return that regulated operators are allowed to make on investments to be taken into account when establishing the regulated access price. [1320] Similarly, in the context of regulated tariffs in the energy sector, WACC has been used as the appropriate rate of return on the capital employed in the regulated activity. [1321] Furthermore, in the context of establishing the compensation for the provision of public service obligations, the WACC of the company entrusted with the provision of the public service has been used as the basis for the calculation of the allowed reasonable profit. [1322]

(1081) Against this background, the Commission is of the view that it is reasonable to use the WACC as a proxy for determining the cost of financing the provision of the Search Data.

(1082) Furthermore, using Alphabet's group WACC as a proxy for the cost of capital employed for the purpose of making the Search Data available, and hence as a proxy for the remuneration of such capital employed, is a reasonable approach for the following reasons.

(1083) In the first place, the sharing of the Search Data is a legal mandate that Alphabet receives as a result of its designation as a gatekeeper in relation to the provision of online search engine services through Google Search. [1323] According to Article 8(1) of Regulation (EU) 2022/1925, Alphabet must ensure and demonstrate compliance with applicable obligations therein, and it must thus bear the costs of such compliance. It follows that Alphabet should in principle not be compensated for any risks deriving specifically from its effective compliance, including, and specially, those that come as a result of the achievement of the goals of the different obligations. In fact, given that increasing contestability in online search engines is the explicit objective of Article 6(11) of Regulation (EU) 2022/1925, it would be unreasonable to allow Alphabet to claim compensation for the potential materialisation of such contestability, and particularly where doing so could undermine, or even neutralise, the intended effect of Article 6(11) of Regulation

---

However, precisely because of the subordinate nature of equity, the cost of equity is higher than the cost of the debt. Hence what matters is the overall WACC of the company and not the cost of the individual WACC components. For instance, in 2025 the group WACC was approximately [...]%, while the cost of debt was below [...]%. Alphabet's reply to RFI 7 of 18 February 2026, Annex Q2.29, Doc ID […]. Furthermore, Alphabet's argument that it is getting penalized for having [description of Alphabet's financial indicators] is not supported by available estimates either, which indicate that [description of Alphabet's financial indicators and comparison to industry standard]. See Damodaran's annual US industry-level cost-of-capital estimates in particular those for the Software (Entertainment) cohort, in which Alphabet is classified. Available at: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datacurrent.html#discrate, Doc IDs […], last accessed on 19 June 2026.

1320 Commission Notice on the calculation of the cost of capital for legacy infrastructure in the context of the Commission's review of national notifications in the EU electronic communications sector (2019/C 375/01), paragraph 3.

1321 Commission decision in State aid SA.35255 (2012/N) – Poland, paragraph 16, footnote 7.

1322 Commission decision in State aid SA.50872 (2020/NN) – Spain – USO compensation to Correos, 2011–2020, paragraph 167.

1323 Google Search is Alphabet's CPS OSE that is subject to the requirement of data sharing in Article 6(11) of Regulation (EU) 2022/1925.

(EU) 2022/1925. Moreover, the Commission notes that Alphabet has been subject to Article 6(11) of Regulation (EU) 2022/1925 at least since its designation in relation to, among other, Google Search, on 5 September 2023. Therefore, any alleged premium for increased market contestability risk is likely to have been already incorporated in the WACC of the group following that date. Accordingly, it does not seem unreasonable to use such group WACC to approximate the reasonable return on the capital employed strictly to comply with its obligations under Article 6(11) of Regulation (EU) 2022/1925.

(1084) In the second place, the Commission received no indication of the availability of any segment-specific WACC to approximate the cost of capital employed for the purpose of sharing the Search Data. [1324] Moreover, Alphabet did not explain, nor provided any relevant evidence thereof, why the cost of the capital employed for providing access to the Search Data is likely to be higher than the WACC required to finance the assets of the group, which Alphabet calculates in the normal course of business.

(1085) In the third place, Alphabet's group WACC reflects the average risk of the portfolio of the group activities, which includes, beyond Google Search, activities that may carry higher risks, such as self-driving cars, data centres, or the development of AI services. Overall, Alphabet's WACC is broadly in line with available aggregate estimates for its industry, which itself remain above the corresponding total-market cost of capital estimate. [1325]

(1086) Against this background, it is reasonable to use the group WACC as a proxy for determining the cost of financing the making of the Search Data available, [description of Alphabet's internal financial information].[1326]

(1087) Furthermore, the addition of a margin reflecting Alphabet's efforts, risks, or investments made in collecting and producing the Search Data should, in principle,[1327] be excluded in the context of Alphabet's FRAND pricing measures under Article 6(11) of Regulation EU 2022/1925 for the following reasons.

(1088) *First*, Alphabet is only obliged to share part of the data it already collects and uses for the purpose of offering its Google Search services.[1328] Alphabet is therefore not required to create any new input (i.e., collect and process additional data) to comply with Article 6(11) of Regulation (EU) 2022/1925. Since this data is non-rivalrous, once generated through users' usage of Google Search services, the fact that eligible beneficiaries access it and use it to optimise their services does not diminish its quantity or quality, remaining available to Alphabet.

(1089) *Second,* recognising a margin designed to reflect the strategic or competitive value of the Search Data, or to compensate Alphabet for potential opportunity costs arising

---

1324 [description of Alphabet's methodology for calculating internal financial information] Alphabet's email of 10 March 2026, Doc ID […].

1325 See recital (1079) in this respect.

1326 In such a case, the group WACC would reflect the alternative uses by Alphabet of the capital employed for the purpose of making the Search Data available.

1327 To the extent that the beneficiary is not an SME, Alphabet may be compensated with an additional margin in the event that (i) it could demonstrate that it would not be able to cover the costs incurred for collecting the relevant data, including a reasonable return, from its own commercial use of that data, or (ii) when an eligible beneficiary operates at a very large scale (i.e., having more than 45 million monthly active end users established or located in the Union and an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years, or an average market capitalisation or equivalent fair market value amounted to at least EUR 75 billion in the last financial year, calculated in line with Article 3(2)(a) and (b) of Regulation (EU) 2022/1925).

1328 See section 4.3.1 on the Parity Principle.

from increased competition, is in principle not coherent with the objectives pursued by Article 6(11) of Regulation EU 2022/1925 of increasing the contestability of online search engines. Remunerating Alphabet with an additional margin would only contribute to further reinforcing the position of Google Search and would risk undermining any additional level of contestability to be achieved. In fact, with a view to maximizing the likelihood of effective take-up of Search Data, and also taking into account the high upfront investments and risks taken by eligible beneficiaries,[1329] limiting compensation to incremental costs, without the inclusion of a margin, for a specific period of time appears most conducive to achieving the objectives of Regulation (EU) 2022/1925, since Article 6(11) of that Regulation is intended to open up an opportunity for eligible beneficiaries to optimise their services and to contest the gatekeeper's search engine.

(1090) *Third,* Alphabet has long been investing in Google Search, including in the collection and processing of user generated data, among which Search Data to be shared under Article 6(11) of Regulation (EU) 2022/1925. Alphabet has [description of Alphabet's financial position based on internal documents]. [1330] In this respect, Alphabet's claim that downstream advertising revenues represent compensation for an entirely different service and that they are legally irrelevant is erroneous.[1331] In the first place, Alphabet monetizes Google Search services through advertising. Alphabet's advertising revenues are therefore inherently relevant to assessing whether Alphabet has been able to recover its investments in that service. [description of Alphabet's internal financial information] [1332] In the second place, in a cost-based context, the way Alphabet monetises Google Search is relevant to ensuring that remuneration does not result in the duplicative recovery of investments already recouped through other revenue streams. [1333]

(1091) Further, Alphabet will likely continue to invest in the collection of Search Data as Alphabet itself is the main user of these data to optimise its own online search engine. If anything, a higher competitive pressure, after many years of lack of contestability, may lead Alphabet to increase its investments in search services. These mitigating factors are similar to the approach currently envisaged under the Data Act, according to which investments that have already been depreciated or covered by other revenue sources should not be taken into account when calculating a potential margin.[1334] In light of this, it is not appropriate, in this context, to award Alphabet a margin to cover its investments in search optimisation or collection of Search Data.

1329 See recital (1042) above.

1330 According to the Designation Decision, Alphabet holds an entrenched position in the OSE market, [description of Alphabet's market position], and its ability to continuously optimise its search technologies on vast user datasets year by year, as well as the significant time and effort required for third-party OSEs to catch up and effectively compete. In addition, as noted in recitals (521) and following, eligible beneficiaries will take time to optimise their services on the basis of Search Data and be able to actually contest Alphabet's position in the search market.

1331 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 508.

1332 See Alphabet's response to RFI PO 1 of 28 January 2026, Annexes Q11.1 Doc ID […], [description of Alphabet's internal financial information].

1333 This claim is also difficult to reconcile with Alphabet's view that SEP valuation constitutes the economically most rigorous framework, since such valuation is premised on the idea that innovation is rewarded by allowing the right-holder to monetise it over a limited period. Where the relevant activity has already generated sustained downstream returns over time, that context may therefore be relevant to assessing whether an investment-recovery component is justified or would risk double recovery. See Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 496.

1334 Importantly, investments that have already been depreciated or recouped through other revenues should not be counted when determining the margin. Draft Compensation Guidelines, section 4.3.2.

(1092) An analysis of the financial performance of Alphabet and the Google Search segment reveals that, at group level, Alphabet has consistently generated sufficient operating cash flows to fund its capital expenditure (Capex) since [description of Alphabet's internal financial information].[1335]

(1093) More specifically, on the basis of financial data provided by Alphabet[1336], the Commission considered a number of financial indicators related to profitability, capital efficiency and cash flow generation.

(1094) *In the first place*, Alphabet's (group-level) operating cash flow has consistently exceeded Capex.[1337] This indicates that the company has generated sufficient internal cash flows to cover its investment needs. In addition, the company has maintained a strong net cash position, with cash and cash equivalents consistently exceeding total debt. Beyond funding its investment needs, since 2015 the company has also returned substantial capital to shareholders through share repurchases, and more recently (since 2024) dividends. Taken together, these factors suggest that the company has not only been able to fund its cumulative investments through internally generated cash flows over time but has also generated surplus cash after reinvesting in the business.

(1095) [description of Alphabet's internal financial information][1338].

(1096) *In the third place*, the Commission considered the return on capital employed ("ROCE")[1339], which measures how efficiently a company uses its capital to generate operating profits. In principle, when ROCE exceeds the WACC, a company is generating returns above its cost of capital. This indicates efficient capital allocation and value creation, as the company earns more on its invested capital than it costs to finance it.

(1097) The Commission found that, [1340] [description of Alphabet's internal financial information]. [1341] In other words, [description of Alphabet's internal financial information] (Figure 16).

Figure 16: Alphabet's ROCE vs. WACC

[image displaying Alphabet's internal financial information]

Source: Commission calculations based on Alphabet financial data

---

1335 Alphabet's reply to RFI 7 of 18 February 2026, Annexes Q1.01, Q1.02 and Q1.03, Doc ID […], Doc ID […], Doc ID […], Doc ID […] and Annexes Q2.12-Q2.25, Doc ID […].

1336 Alphabet provided its Form 10-k and relevant amendment filings from FY 2004 to 2025, the Amendment No. 4 to Form S-1 Registration Statement, quarterly global Search P&L data as prepared in the ordinary course of business from Q2 2019 until Q4 2025, yearly Search P&L data for years 2014 to 2019, as well as the group-level WACC from 2015. [description of Alphabet's methodology for calculating internal financial information] Alphabet's response to RFI PO 1 of 28 January 2026, Annexes Q11.1 Doc ID […]. Alphabet's reply to RFI 7 of 18 February 2026, Annexes Q1.01–Q1.03, and Q2.01–Q2.32, Doc ID […], Doc ID […], Doc ID […], Doc ID […], Doc ID […] and Doc ID […].

1337 Data for the purpose of this comparison is available since [...].

1338 [description of Alphabet's internal financial information].

1339 ROCE for a given year is calculated by dividing the operating profit (post-tax) by the average Capital employed of the same and the preceding year. Capital employed is the difference between Total assets and Current liabilities.

1340 The Commission relied on the WACC (post-tax) based on the 10-year horizon, as this series covers a longer period. The reported WACC based on the 20-year horizon extends back only to 2019. In any event, the overall conclusions are not affected by the choice of WACC, as the WACC remains consistently below ROCE under either metric.

1341 [description of Alphabet's internal financial information].

(1098) [description of Alphabet's internal financial information], the Commission estimated conservatively a ROCE for Google Search by assuming that the total group capital base is attributed to the Google Search segment. Hence, the Google Search ROCE is obtained by dividing the Google Search operating profit[1342] by the total group capital employed, which likely understates the segment's true capital efficiency. [description of Alphabet's internal financial information] (Figure 17)[1343].

Figure 17: Google Search segment's ROCE vs. group-level WACC

[image displaying Alphabet's internal financial information]

Source: Commission calculations based on Alphabet financial data

(1099) *Fourth,* since Alphabet is only required to share the specific elements of user interaction data that it collects in the normal course of business, Alphabet will always retain a unique advantage as compared to eligible beneficiaries. In particular, Alphabet will always retain more user interaction data than it will share with third parties as the Search Data and, as a result, it will always have the possibility to extract better insights into its users' behaviour and interactions than the eligible beneficiaries accessing the Search Data. Moreover, limiting the obligation to anonymized data translates in a further reduced usability of the Search Data compared to the pool of user data interactions that is available to Alphabet on a rolling basis.

(1100) *Fifth,* the Search Data is only data generated by the interactions of end users and business users on Google Search without it having been processed or analysed by the search technology, including algorithms, that Alphabet uses to optimise its own search services.

(1101) Against this background, the Commission considers that FRAND compensation under Article 6(11) of Regulation (EU) 2022/1925 must be confined to the recovery of access-related costs and a reasonable return, which corresponds to a return on the capital employed for the purpose of the provision of access to Search Data that must not exceed Alphabet's WACC.

4.5.3.4. Limitations to Alphabet's cost-based pricing measures under Article 6(11) of Regulation (EU) 2022/1925

(1102) As outlined in section 4.5.3.1, the FRAND nature of the pricing measures specified under Article 6(11) of Regulation (EU) 2022/1925 should be assessed in light of the specific objectives of that provision, the broader objectives of fairness and contestability, and the specific circumstances in which the pricing measures are specified.

(1103) As such, the Commission considers that while the objectives of Article 6(11) of Regulation EU 2022/1925, as well as those of that regulation more generally, continue to apply, there are certain circumstances that may limit the application of the pricing measures specified for Alphabet in section 4.5.2. Under such circumstances, Alphabet may be allowed a remuneration above the price strictly based on the incremental costs of providing access to Search Data including a reasonable return on the capital employed for the purpose of making the Search Data available, which must not exceed Alphabet's WACC.

1342 Despite this being segment result, a post-tax operating profit was calculated and used for the current comparison for consistency reasons.

1343 [description of Alphabet's internal financial information].

(1104) *First*, when an eligible beneficiary operates at a very large scale, Alphabet may be entitled to an additional margin, which however cannot exceed the operating margin (in percentage terms) of Alphabet's Google Search business. Undertakings are qualified as operating at very large scale in this context, if they have more than 45 million monthly active end users established or located in the Union and an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years, or an average market capitalisation or equivalent fair market value amounted to at least EUR 75 billion in the last financial year, calculated in line with Articles 3(2)(a) and (b) of Regulation (EU) 2022/1925. Such eligible beneficiaries may be considered as having already achieved significant scale and relevance for end users in the provision of online search engines services,[1344] as well as a solid financial position.

(1105) *Second,* when an eligible beneficiary is also a designated gatekeeper under Article 3(4) Regulation (EU) 2022/1925 in relation to the provision of an online search engine core platform service, Alphabet may deviate from the FRAND pricing specified. In that case, Alphabet must negotiate, in good faith, pricing terms with eligible beneficiaries, provided that any resulting terms remain FRAND, taking into account the relevant circumstances, in line with the interpretation under Article 6(11) of Regulation (EU) 2022/1925 set out in section 4.5.3.1. Under these circumstances, both Alphabet and the eligible beneficiary would be operating at a comparable scale and would therefore be in a more balanced position to freely negotiate a FRAND compensation for accessing the Search Data.

(1106) *Third*, provided that such beneficiaries do not qualify as SMEs,[1345] where Alphabet could credibly demonstrate that it would not be able to cover the costs of collecting the relevant data, including a reasonable return on capital from its own commercial use of that data,[1346] Alphabet may also be entitled to a margin within the same limits as laid out in recital (1104) above. This is justified in light of the need to ensure that Alphabet remains able to continue providing its own services, without however creating or maintaining an unfair advantage.

4.6. Measures relating to process for Search Data acquisition and pre-acquisition data testing

4.6.1. Introduction

(1107) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to grant access to Search Data on FRAND terms. The Commission has specified in this Decision certain elements of the data sharing process that are essential to ensuring that terms are FRAND. The Commission also intends this process to enable Alphabet to implement the technical, organisational, contractual and governance measures for anonymisation of personal data specified at section 4.4.4.

(1108) A FRAND process for data acquisition is necessary to ensure that Alphabet does not apply a data acquisition process that unfairly, unreasonably or discriminatorily denies

---

1344 Recital 61 DMA establishes that the value of online search engines to their respective business users and end users increases as the total number of such users increases.

1345 With a view to facilitating take-up of the data access under this provision, SMEs should benefit from additional protection from excessive economic burdens.

1346 The revenue from Alphabet's commercial use of the data should at least include Google Search revenue, which is defined in this context as any revenue directly or indirectly attributable to the provision, operation, or monetisation of the Google Search service, including revenues generated through search advertising, intermediation of search-related traffic, and any other commercial activities deriving value from search queries or search-related user interactions.

or delays access to the Search Dataset, or makes such access ineffective. At the same time, such a FRAND process must enable Alphabet to apply the contractual measures specified at section 4.4.4.2.

(1109) The Commission therefore specifies the following elements of the process:

(a) Process and practical arrangements for pre-acquisition data testing;

(b) Process for finalising the Search Dataset;

(c) Process for finalising the licence agreements for the Search Dataset and test data samples;

(d) Process for making the Search Dataset available, reviewing eligibility of undertakings applying for eligibility, finalising pricing terms and ensuring continuity of access;

(e) Processes for refusing, suspending and terminating access to the Search Dataset;

(f) Requirement to impose financial penalties in exceptional circumstances; and

(g) Requirement to amend documents and obligation to inform the Commission and data protection supervisory authorities of decisions refusing, suspending, restoring or terminating access to the Search Dataset.

4.6.2. The gatekeeper's view

(1110) Alphabet's views on the processes for Search Data acquisition and pre-acquisition technical testing under the Preliminary Findings were set out in its response to the Preliminary Findings[1347] and in its submission on contractual measures.[1348] Alphabet provided this submission on contractual measures several weeks after its response to the Preliminary Findings. That submission contained more detailed views on the processes specified in this section, as well as the contractual measures specified in section 4.4.4.2 and the eligibility measures specified in section 4.2.2. It also suggested some concrete changes to address some of Alphabet's concerns. Alphabet's views expressed in its response to the Preliminary Findings and in its submission on contractual measures are set out in the coming recitals.

(1111) **Regarding the process for finalising the Search Dataset (section 4.6.4.2),** Alphabet argued that the implementation deadline was too short.[1349] It complained that the Preliminary Findings would require Alphabet to finalise six separate workstreams, namely:

(a) Building new infrastructure to make the Search Dataset available;

(b) Collecting and deriving datapoints;

(c) Restructuring the Search Dataset;

(d) Building an anonymisation process;

(e) Drafting new contracts; and

(f) Developing a new pricing framework.

(1112) In this regard, it relied on the view expressed in the Expert Report on Anonymisation that implementing proposed anonymisation measures (workstream (d) in the above

1347 Alphabet's response to the Preliminary Findings, Doc ID [...].

1348 Alphabet's submission on contractual measures, Doc ID […].

1349 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 548

list) would take between three and four months and stated that since anonymisation was only one of these six workstreams, a three-month deadline for finalising the Search Dataset was disproportionate.[1350] Alphabet further submitted that, in the Commission's decision in case DMA.100203,[1351] Apple Inc. was granted nine months to implement certain changes and additional time to implement others.[1352]

(1113) **Regarding submission of level 2 assurance reports to maintain access to the Search Dataset (section 4.6.6.3.2),** Alphabet argued that the intervals between audits (15 months between the first Level 1 and first Level 2 reports and 12 months between all subsequent Level 2 reports) specified in the Preliminary Findings were excessive.[1353] Alphabet argued that this would leave periods during which misuse would not be detected and argued that Alphabet should have the right to trigger an interim audit if it had a reasonable, good faith belief that the third-party OSE was breaching contractual measures.[1354] In Alphabet's submission on the Revised Measures, it argued that the period between submission of the first Level 1 and first Level 2 reports should be reduced to six months.[1355] Alphabet also complained that the Preliminary Findings placed undue trust in third-party OSEs' incentives to abide by contractual measures.[1356]

(1114) **Regarding processes for refusing, suspending and terminating access to the Search Dataset (section 4.6.7),** Alphabet argued that it should have the right to suspend and terminate for copying Alphabet's search algorithms, index or results and for material breaches of contract or failure to comply with applicable law.[1357]

(1115) It submitted the Preliminary Findings placed the burden on Alphabet to confirm data erasure without granting it the practical means to verify or enforce this requirement.[1358] To remedy this, it argued that it should have the right, at its own expense, to appoint an auditor to verify erasure.[1359]

(1116) Regarding changes of control, Alphabet asserted that the Preliminary Findings would only require the change to be notified and submission of a Level 1 reasonable assurance report after a change of control takes effect.[1360] It argued that Alphabet should have the right to suspend or terminate access pending submission of a Level 1 reasonable assurance report taking the change of control into account.

(1117) **Regarding the requirement to impose financial penalties in exceptional circumstances (section 4.6.8.2)**, Alphabet argued that contractual financial penalties would be legally unenforceable in certain jurisdictions, namely Ireland (which is a Member State of the Union) and the United Kingdom (which is not a Member State

---

1350 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 550; Expert Report on Anonymisation, Doc ID […], paragraph 328.

1351 DMA.100203 – Apple – Operating systems – iOS – Article 6(7) – SP – Features for Connected Physical Devices

1352 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 551.

1353 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 576 and 578.

1354 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 295(b) and 576; and Alphabet's submission on contractual measures, Doc ID […], pages 2 and 16.

1355 Alphabet's response to the Revised Measures, Doc ID […], paragraph 119.

1356 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 288 – 289.

1357 Alphabet's submission on contractual measures, Doc ID […], pages 20 and 21.

1358 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 580(d).

1359 Alphabet's submission on contractual measures, Doc ID […], pages 4 and 21 – 22.

1360 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 580(1); and Alphabet's submission on contractual measures, Doc ID […], page 19. These assertions are incorrect: see paragraphs 127 (a) and (b) of the Annex to the Preliminary Findings.

of the Union).[1361] It argued that Alphabet should have the right to seek damages against a third-party OSE for losses Alphabet incurred resulting from breaches of contract by that third-party OSE.[1362]

4.6.3. Process and practical arrangements for pre-acquisition technical testing

4.6.3.1. Introduction

(1118) Third-party OSEs, before accessing the full dataset, do not have the same visibility that Alphabet has on the format, content and scope of the Search Dataset. To ensure that third-party OSEs have access to the Search Dataset on FRAND terms, third-party OSEs need access to limited samples of the Search Dataset ("**test data samples**") before eventually agreeing to acquire the Search Dataset. The purpose of test data samples is to allow third parties to conduct technical tests and make an informed decision regarding whether they wish to acquire the Search Dataset.

(1119) Alphabet currently offers small samples of Google Search Data to potential recipients to allow them to conduct technical testing and decide whether they wish to acquire access to the dataset. Alphabet offers two types of test data sample:

(a) A 1000-row sample of 58 unique queries offered free of charge (the "**small Alphabet sample**"). The small Alphabet sample is not subject to any maximum retention period. Alphabet transfers the small Alphabet sample to third-party OSEs via Excel file over e-mail;[1363] and

(b) A one-time 5% sample of a quarterly dataset (i.e., potentially several billion queries),[1364] taken either at EEA- or country-level, available to be downloaded (the "**large Alphabet sample**"). Alphabet charges a fee for the large Alphabet sample on the same basis described in section 1.2 and requires third-party OSEs to sign the licence agreement described at section 1.2. The large Alphabet sample is subject to the same security and data protection provisions and 365-day maximum retention period as data shared under Alphabet's European Search Dataset Licensing Program.[1365]

(1120) While [1-10] third-party OSEs have thus far taken up the offer of the small Alphabet sample, only a single third-party OSE has opted to acquire the large Alphabet sample.[1366]

(1121) The Commission agrees with Alphabet that test data samples are required for the effectiveness of the present data sharing scheme. However, as further explained in section 4.6.3.3, the Commission is of the view that there are certain deficiencies in Alphabet's current offer of test data samples. For instance, while the Commission agrees that Alphabet must enable data testing before a third-party OSE agrees to acquire the Search Dataset, the small Alphabet sample is too small on its own to enable meaningful data testing and must be complemented by another test data sample before a third-party OSE undergoes an independent assurance audit.

1361 Alphabet's submission on contractual measures, Doc ID […], page 23.

1362 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 581; and Alphabet's submission on contractual measures, Doc ID […], pages 22 – 23.

1363 Alphabet's reply to RFI of 12 February 2026, Doc ID […], question 1

1364 In Q4 2023 in the EEA, Alphabet received approximately [number] queries. 5% of these is approximately [number] queries. See Alphabet's reply to RFI of 22 December 2023, Doc ID […], question 1.d

1365 Alphabet's reply to RFI 12 of February 2026, Doc ID […], question 1.

1366 Alphabet's reply to RFI 12 of February 2026, Doc ID […], question 2.

(1122) The Commission therefore has specified in this Decision the measures that Alphabet must implement to make appropriate test data samples available to third-party OSEs and allow them to make an informed choice on whether they wish to acquire the Search Dataset.

4.6.3.2. Measures

(1123) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must give third-party OSEs the opportunity to conduct technical testing on test data samples before they agree to acquire the Search Dataset.

(1124) Alphabet must provide three different test data samples to any eligible third-party OSE applying for eligibility to test data samples or the Search Dataset. Each test data sample must have a different scope in terms of content as well as means and conditions of access. These are:

(a) **Sample A:** Alphabet must continue to provide a small sample of 1 000 rows (i.e., 58 unique queries) from the Search Dataset;

(b) **Sample B:** Alphabet must provide a synthetic dataset that eligible third-party OSEs may download onto their own servers to conduct technical testing; and

(c) **Sample C:** Alphabet must provide a large representative sample dataset that eligible third-party OSEs may download onto their own servers to conduct technical testing.

4.6.3.2.1. Sample A – access arrangements, access conditions and content

(1125) Alphabet must continue to provide a 1 000-row sample (i.e., 58 unique queries) of the Search Dataset free of charge ("**Sample A**"). Alphabet must continue to allow third-party OSEs to download Sample A onto their own servers free of charge. Alphabet may impose a contractual restriction preventing the third-party OSE from sharing Sample A with any other person or undertaking.

(1126) Alphabet must otherwise make Sample A available under the same conditions it makes the small Alphabet sample available.

4.6.3.2.2. Sample B – access arrangements, access conditions and content

(1127) Alphabet must prepare a synthetic dataset of 10 million individual representative artificially generated unique queries (also often called "synthetic" queries) and metadata ("**Sample B**") and provide this to any third-party OSE that requests it. Alphabet must comply with any request from a third-party OSE that the copy of Sample B it receives contain a particular number of queries and associated metadata, up to a maximum of 10 million individual queries.

(1128) Alphabet must allow third-party OSEs to download Sample B onto their own servers. Alphabet may impose a contractual restriction preventing the third-party OSE from sharing Sample B with any other person or undertaking.

(1129) Alphabet must not make access to Sample B conditional on the third-party OSE in question providing any assurance report specified in section 4.4.4.2.4.1 or undergoing an audit associated with this assurance report. Alphabet may only grant Sample B to a third-party OSE that it has deemed a third-party OSE eligible to receive the Search Dataset in accordance with section 4.2.2.

(1130) Alphabet must explain, in a clear and transparent manner, the method by which it produced Sample B. Alphabet must ensure that Sample B is a faithful representation

of the real Search Dataset to which technical measures specified in section 4.4.4.1.1 have been applied. This means, among other things, that Sample B must:

(a) Accurately resemble the real Search Dataset in content and form;

(b) Faithfully reflect the relationship between queries and metadata;

(c) Include all the data fields specified in section 4.3.2; and

(d) Have the technical measures specified in section 4.4.4.1.1 applied in the same way they would be applied to the real Search Dataset.

(1131) Alphabet may limit the time during which third-party OSEs may retain Sample B. This retention period must be a period of at least three months from the date on which Sample B was first made available to that third-party OSE.

(1132) Alphabet may charge third-party OSEs a fee for accessing Sample B. This fee must be calculated using the method specified in section 4.5.2.

4.6.3.2.3. Sample C – access arrangements, access conditions and content

(1133) Alphabet must provide a sample of 5% of the final Search Dataset selected from queries occurring in no less than one month and no more than one year ("**Sample C**") (with the exact period to be specified by the third-party OSE requesting Sample C).

(1134) Alphabet must provide Sample C once the Search Dataset is finalised in accordance with section 4.6.4.2 and all applicable conditions for the sharing of the Search Dataset have been met by the third-party OSE. Alphabet must require third-party OSEs to apply the retention period specified in section 4.4.4.2.1.1 to Sample C.

(1135) Alphabet may charge third-party OSEs a fee for accessing Sample C. This fee must be calculated using the method specified in section 4.5.2.

(1136) Alphabet must comply with any requests from any third-party OSE that all queries in the Sample C dataset it accesses:

(a) Come from a particular Member State or Member States of the Union;

(b) Be in a particular language or languages; or

(c) Take place within a particular period of no less than one month.

4.6.3.3. The Commission's assessment

(1137) Article 6(11) of Regulation (EU) 2022/1925 requires gatekeepers to provide third-party OSEs with access to the Search Dataset on FRAND terms. That Article also requires that any data constituting personal data that Alphabet shares be anonymised.

(1138) Transparency is a key element of a FRAND process for data acquisition. Pre-acquisition testing will enable third-party OSEs to examine the content, quality and utility of the Search Dataset. As one market participant explained, pre-acquisition testing will allow third-party OSEs to verify the completeness/schema of the Search Dataset and check for unexpected issues.[1367] For these reasons, such testing is necessary to ensure access to the Search Dataset on FRAND terms.

(1139) The acquisition of the Search Dataset will require significant investments from third-party OSEs. Test data samples will allow third-party OSEs to assess whether they wish to acquire the Search Dataset before making these investments. It would be

[1367] [market participant's] email to the Commission of 18 March 2026, Doc ID […].

both unfair and unreasonable to require third-party OSEs to decide on these investments with no insight into the Search Dataset's exact scope, format and quality, while Alphabet retains full information on the Search Dataset's scope, format and quality.

(1140) Alphabet itself has recognised that testing is a necessary component of access to the Search Dataset on FRAND terms, given that it offers the small Alphabet sample and the large Alphabet sample to third-party OSEs.

(1141) However, market participants indicate that Alphabet's practices around sharing the Search Dataset do not satisfy those participants' needs. The small Alphabet sample of 58 queries is far smaller than the minimum size test data sample any consulted market participant stated it required. All consulted market participants stated that they needed to access a test data sample comprising at least several thousand unique queries, and most required a test data sample of 1 million or more, with two market participants stating that they required approximately 10 million unique queries.[1368]

(1142) Sample A, Sample B and Sample C are necessary to ensure that the test data samples Alphabet offers are useful for third-party OSEs, while reflecting the data scope and technical and contractual measures specified in this Decision.

4.6.3.3.1. Commission's assessment – Sample A

(1143) Although the small Alphabet sample is far smaller than market participants require, the Commission sees benefit in Alphabet continuing to make a similar sample available (i.e., Sample A) alongside Sample B and Sample C. Sample A will allow third-party OSEs to conduct a brief initial check to verify the contents of the Search Dataset in terms of data scope and format. Moreover, Alphabet will be able to easily confirm that Sample A contains no end user personal data and can therefore share Sample A without requiring a third-party OSE to implement the contractual and independent verification measures specified in section 4.4.4.2.

4.6.3.3.2. Commission's assessment – Sample B

(1144) **First,** it is appropriate to require Alphabet to make a test data sample of 10 million queries available for third-party OSEs to download onto their own servers before undergoing an audit.

(1145) Under section 4.4.4.2.4.1, third-party OSEs will need to submit to an extensive audit before they can receive the Search Dataset. To successfully obtain a Level 1 assurance report following this audit, a third-party OSE may need to incur costs and make changes to its business, which may require financial and organisational commitments.

(1146) Without effective access to a sample of the Search Dataset, third-party OSEs may lack information to determine whether such investments are commercially worthwhile. It is FRAND to enable third-party OSEs to make an informed decision about whether they wish to access the Search Dataset before undergoing such an audit. To guarantee FRAND access, third-party OSEs must have sufficient information to determine whether they wish to acquire the Search Dataset, the volume of the Search Dataset they wish to acquire, the kinds of investments and

[1368] See: [market participant's] reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's] reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to Question 1 of RFI 12 February 2026, Doc ID […]; and [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1.

changes they will need to make within their own businesses and the exact uses to which they will put the Search Dataset in order to optimise their search algorithms.

(1147) Third-party OSEs can only properly make this assessment if they can run tests on a data sample of several million individual queries that reflects the richness and complexity of the Search Dataset stored on their own servers.

(1148) As explained, most consulted market participants required a test data sample of 1 million or more unique queries, with two market participants stating that they required approximately 10 million unique queries.[1369] Moreover, all consulted market participants expressed a need and/or clear preference for being able to access such a test data sample on their own servers.[1370] Only one market participant was open to the idea of accessing a test data sample on Alphabet's server, stating that it may be sufficient to access a test data sample on Alphabet's server provided it could manipulate data on Alphabet's servers as part of technical tests to assess whether it was worth acquiring the Search Dataset.[1371]

(1149) Sample B will allow third-party OSEs to download several million queries of a dataset that accurately represents the richness and complexity of the Search Dataset onto their own servers. They can thereby conduct meaningful technical testing before deciding to undergo the independent assurance audit.

(1150) **Second,** it is necessary to require Alphabet to ensure that Sample B is synthetic. Section 4.4.4.2.1.1 requires that Alphabet remain the controller of end users' personal data at all times before third-party OSEs receive access to the Search Dataset. Under section 4.6.6.1.2, Alphabet must not allow third-party OSEs to access the Search Dataset before:

(a) Alphabet has deemed those third-party OSEs to be third-party OSEs eligible to receive the Search Dataset; and

(b) Those third-party OSEs have submitted a Level 1 reasonable assurance report.

(1151) Third-party OSEs will be able to access Sample B without fulfilling either of these criteria. Sample B will be a synthetic dataset containing no end user personal data and can therefore be downloaded onto third-party OSEs' own servers. This will allow third-party OSEs to conduct necessary testing on their own servers without breaching the requirement that Alphabet remain the controller of any personal data.

(1152) As set out above, most market participants consulted wished to download several million queries onto their own servers without first providing a Level 1 assurance report (i.e., proving their implementation of the contractual measures at section 4.4.4.2).

(1153) Moreover, the Commission considers that once the algorithm for producing the synthetic data forming part of Sample B has been trained, there should be no

---

1369 See: [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's] reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; and [market participant's] reply to RFI 12 February 2026, Doc ID […], question 1.

1370 See: [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1; and [market participant's]reply to RFI 12 February 2026, Doc ID […], question 1.

1371 See: [market participant's] reply to Question 1 of RFI 12 February 2026, Doc ID […], question 1.

additional cost or complexity for Alphabet to produce a sample of several million queries (versus producing a smaller sample of, e.g., several thousand).

(1154) **Third**, it is necessary to require Alphabet to ensure that Sample B faithfully represents the Search Dataset and to explain the method under which it produced Sample B in a clear and transparent manner.

(1155) Because Sample B will be synthetic, to ensure it remains truly useful for third-party OSEs, it should faithfully represent the Search Dataset in a way that allows them to conduct meaningful testing and to verify the completeness of the Search Dataset. Moreover, to ensure FRAND access, Alphabet must ensure that it is transparent regarding the methodology used to generate Sample B. These requirements are supported by the views of market participants, one of which stated that a synthetic dataset should *"be genuinely random and representative, with transparency on the sampling methodology…."*[1372]

(1156) **Fourth**, the measures relating to prices and fees for Sample B are also necessary to ensure FRAND access to the Search Dataset. Alphabet will be entitled to charge fees for Sample B calculated on the same basis as the Search Dataset, as specified in section 4.5.2. For the reasons given in section 4.5.3, this pricing method is necessary to ensure access on FRAND terms. For the avoidance of doubt, the fee that Alphabet can charge for Sample B should not be double counted in the fee applicable to the Search Dataset.

4.6.3.3.3. Commission's assessment – Sample C

(1157) **First,** Sample C is necessary to provide third-party OSEs with FRAND access to a sizeable sample of the Search Dataset, before concluding a licensing contract for the Search Dataset, to further test:

(a) The utility of the Search Dataset; and

(b) The suitability of the third-party OSE's data processing infrastructure to receive and process the Search Dataset.

(1158) After obtaining a Level 1 reasonable assurance report, third-party OSEs will have to make certain further investments to acquire the Search Dataset.

(1159) They therefore require sufficient information to determine whether final investments in the Search Dataset and data processing infrastructure are worthwhile, which can be made more fully with access to a non-synthetic sample of the Search Dataset allowing third-party OSEs to test use cases under real conditions. Sample C is necessary to allow third-party OSEs to make such an informed decision. It is therefore appropriate to require Alphabet to share Sample C with third-party OSEs that submit a Level 1 reasonable assurance report.

(1160) **Second,** it is justified to limit the requirement to make Sample C available to those that are eligible third-party OSEs and prove that they have implemented applicable contractual measures by submitting a Level 1 reasonable assurance report. As required by sections 4.2.2, 4.4.4.2 and 4.6.6.1.2, Alphabet may only share the Search Dataset with a third-party OSE that has fulfilled these criteria.

(1161) **Third**, Sample C is essentially the same as the large Alphabet sample. It would be unfair and unreasonable for Alphabet to deny third-party OSEs access to Sample C at a future point, given that Alphabet already provides a very similar test data sample. Such a move would also be discriminatory as it would treat future requests from

[1372] [market participant's] email to the Commission of 18 March 2026, Doc ID […].

third-party OSEs differently to third-party OSEs requesting testing samples at present.

(1162) **Fourth**, the measures relating to prices and fees for Sample C are also necessary to ensure FRAND access to the Search Dataset. Alphabet will be entitled to charge fees for Sample C calculated on the same basis as the Search Dataset, as specified in section 4.5.2. For the reasons given at section 4.5.3, this pricing method is necessary to ensure access on FRAND terms.

4.6.4. Process for finalising the Search Dataset

4.6.4.1. Introduction

(1163) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. It also requires that any data in the Search Dataset which is personal data be anonymised. The Commission therefore has specified in this Decision a time limit for finalising the Search Dataset that is fair and reasonable.

4.6.4.2. Measures

(1164) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must finalise the Search Dataset as soon as possible and no later than four months after the Commission's adoption of this decision. Alphabet must notify the Commission as soon as it has finalised the Search Dataset. This notification shall describe the actions Alphabet has taken to implement the measures specified in sections 4.3.2, 4.3.3 and 4.4.4.1.1.

(1165) Within four months of the adoption of these measures, Alphabet must share a document with the Commission setting out:

(a) The final latency of Search Data sharing along with the technical description and justification, as specified in section 4.3.3.2.2; and

(b) The information on personal data detectors and list of result types specified at section 4.4.4.1.1, recital (609).

4.6.4.3. The Commission's assessment

(1166) Procedural transparency is a key element of a FRAND process for data acquisition. Time limits are a key element of procedural transparency. Time limits ensure access on FRAND terms, as they allow third-party OSEs to allocate and adequately plan time and resources for Search Dataset acquisition and the implementation of measures to ensure anonymisation.

(1167) A key aim of the EU legislature in creating an immediately applicable *ex ante* obligation under Article 6(11) of Regulation (EU) 2022/1925 was to ensure timely compliance.[1373] Alphabet was designated as a gatekeeper in respect of its OSE CPS on 5 September 2023[1374] and was required to comply with Article 6(11) of Regulation (EU) 2022/1925 within six months of that date (i.e., by 4 March 2024).[1375] Alphabet has therefore had over two years to prepare the Search Dataset in compliance with Article 6(11) of Regulation 2002/1925.

1373 Commission Staff Working Document, Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector, COM (2020) 842 final, part 1, pages 61 – 62 and 96 – 97.

1374 See: Commission decision in DMA.100004 - *Alphabet - online search engines*.

1375 Article 3(10) of Regulation (EU) 2022/1925.

(1168) However, the Commission recognises that the anonymisation measures that it has specified will require significant modifications to the Search Dataset. Alphabet will need a reasonable period to implement these.

(1169) In the Commission's view, a period of four months constitutes such a reasonable period for finalising the Search Dataset. In the Preliminary Findings, the Commission specified a period of three months by the end of which Alphabet would be required to implement these measures. This was based on the Expert Report on Anonymisation, which states that: "*Our proposed anonymisation procedure is relatively complex, but can be split into small components, and is much simpler than many routine operations of Google products. We believe that it could be implemented and deployed to production in about 3-4 months.*"[1376] As noted above, in its response to the Preliminary Findings, Alphabet itself relied on this statement from the Expert Report.[1377]

(1170) This time limit is further supported by Alphabet's own actions in responding to Commission requests for information. For instance, on 26 March 2025, the Commission requested a sample of search data. Alphabet provided this sample across two tranches on 28 May 2025 and 20 June 2025 (i.e., within significantly less than four months).[1378] Moreover, on 11 February 2026, the Commission requested Alphabet to add further parameters to this dataset.[1379] Alphabet responded that it required nine weeks (i.e., approximately two months) to add the most complex of these parameters to the dataset.[1380]

(1171) Alphabet will benefit from work already undertaken to comply with Commission requests for information. It will also have been able to conduct advanced preparatory anonymisation work for producing the Search Dataset based on the Commission's Preliminary Findings and subsequent meetings held with the Commission to discuss anonymisation.

(1172) The Commission however notes Alphabet's submissions that it may require some additional time to finalise the Search Dataset. In its final measures, the Commission has therefore increased the time limit within which Alphabet will have to finalise the Search Dataset to four months (the upper limit of the estimate given in the Expert Report, which Alphabet itself relied on in its response to the Preliminary Findings).

(1173) The Commission acknowledges that Alphabet will have to undertake multiple workstreams to prepare the Search Dataset for sharing. However, it is implausible, as Alphabet appears to suggest in its response to the Preliminary Findings, that Alphabet would undertake each of these workstreams sequentially. Alphabet is one of the world's largest corporations. Each of the six workstreams identified by Alphabet at paragraph 548 of its response to the Preliminary Findings can be undertaken by different dedicated teams within Alphabet's organisation, with the help of external service providers if needed. This means that they can all be done concurrently, rather than sequentially. The fact, for instance, that members of Alphabet's legal team will have to draft template licence agreements has no bearing on the ability of Alphabet's engineering teams to prepare the Search Dataset by applying the technical measures specified in section 4.4.4.1.1. Likewise, the

1376 Expert Report on Anonymisation, Doc ID […], paragraph 328.
1377 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 550.
1378 See: Alphabet's reply to RFI of 26 March 2025, Doc ID […], question 1.
1379 RFI to Alphabet of 11 February 2025, Doc ID […].
1380 Alphabet counsel's email to the Commission of 16 February 2026, Doc ID […].

Commission expects that Alphabet has the resources to dedicate a separate technical team to building data sharing infrastructure.

(1174) Finally, contrary to Alphabet's submission, the time limits specified in case DMA.100203 are irrelevant to the present proceedings. That decision concerned the obligation on gatekeepers to ensure effective interoperability under Article 6(7) of Regulation (EU) 2022/1922 and is moreover confined to its own facts.

(1175) The Commission therefore concludes that the time limit for finalising the Search Dataset is justified and necessary to comply with Alphabet's obligation to provide the Search Dataset on FRAND terms.

4.6.5. Process for finalising the licence agreements for the Search Dataset and the test data samples

4.6.5.1. Introduction

(1176) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to grant access to the Search Dataset on FRAND terms. Alphabet presently provides the Search Dataset and the large Alphabet sample under a template licence agreement.[1381] However, Alphabet will need to prepare new template licence agreements for each of the Search Dataset, Sample A, Sample B and Sample C that reflect changes required by the measures the Commission has specified in this Decision.

(1177) The Commission has therefore specified in this Decision a process for finalising these template licence agreements that ensures access to the Search Dataset and test data samples on FRAND terms.

4.6.5.2. Measures

(1178) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must prepare a template licence agreement for the sharing of the Search Dataset with third-party OSEs, implementing all applicable provisions of the measures specified, within two months of the Commission's adoption of this Decision.

(1179) Alphabet must also prepare template licence agreements for sharing Sample A, Sample B and Sample C within two months of the Commission's adoption of this Decision.

(1180) Within one working day of finalising the template licence agreements, Alphabet must share a copy of each template licence agreement with any undertaking applying for eligibility, eligible third-party OSEs and the Commission.

(1181) The Search Dataset and Sample C template licence agreements must allow a third-party OSE to specify that all queries forming part of the Search Dataset or Sample C dataset it receives come from a particular Union Member State or Member States, be in a particular language or take place within a period of no less than one month.

(1182) Alphabet may only impose conditions for sharing the Search Dataset or test data samples that are FRAND and strictly proportionate. These conditions must not impede in any way the effectiveness of this Decision or the specified measures.

4.6.5.3. The Commission's assessment

(1183) The availability of an appropriate template licence agreement is essential to ensure that the terms on which Alphabet offers the Search Dataset are FRAND. Sharing the template licence agreement with both requesting third-party OSEs and the

[1381] Alphabet's reply to RFI dated 15 May 2024, Doc ID […], question 1; and Annex Q1 to Alphabet's reply to RFI dated 15 May 2024, Doc ID […].

Commission will create transparency and allow all parties to satisfy themselves that Alphabet is effectively complying with Article 6(11) of Regulation (EU) 2022/1925.

(1184) A time limit of two months to prepare the template licence agreements is justified. Third-party OSEs should have the opportunity to review template licence agreements well in advance of receiving access to test data samples and the Search Dataset, so they can plan within their organisations and allocate resources. At the same time, Alphabet must be given an opportunity to prepare a template licence agreement which reflects the detailed measures specified in this Decision. Any additional conditions included in the template licence agreements should be FRAND and should not in any way impede or reduce the effectiveness of the measures specified in this Decision.

(1185) The Commission's view is that a timeframe of two months is adequate to allow Alphabet to prepare the template licence agreements, given that a pre-existing licence agreement already exists and that this Decision provides detailed guidance.

(1186) The Commission therefore concludes that the measures specified at section 4.6.5.2 are necessary to enable the sharing of the Search Dataset on FRAND terms.

(1187) In relation to Alphabet's obligation under recital (1180) to share its template licence agreements with the Commission, eligible third-party OSEs and undertakings applying for eligibility, the Commission will assess the full template licence agreements including all contractual provisions. This assessment will take into account the feedback of interested third parties and will be conducted in view of the requirements of Article 6(11) of Regulation (EU) 2022/1925 and of the measures set out in the present Decision.

4.6.6. Processes for making the Search Dataset available, reviewing eligibility of undertakings applying for eligibility, finalising pricing terms and ensuring continuity of access

4.6.6.1. Process for providing Search Dataset(s) and reviewing eligibility of undertakings applying for eligibility

4.6.6.1.1. Introduction

(1188) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms.

(1189) To take into account the measures specified at sections 4.2.2 and 4.4.4.2, the Commission has specified in this Decision a process for providing the Search Dataset and reviewing eligibility which is FRAND.

4.6.6.1.2. Measures

(1190) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must engage with any undertaking applying for eligibility to determine whether it is eligible to receive the Search Dataset.

(1191) Alphabet must put in place a structured, adequately documented process setting out how it will receive, acknowledge, assess and respond to applications for eligibility, requests for the Search Dataset and test data samples.

(1192) To this end, within 45 days of the adoption of these measures, Alphabet must provide a publicly accessible webpage containing up-to-date information including:

(a) A clear explanation of Alphabet's obligations under Article 6(11) of Regulation (EU) 2022/1925 specified in this Decision; and

(b) Clear and detailed information on how to contact Alphabet with a view to submitting a request for the Search Dataset.

(1193) Alphabet must reply to any expressions of interest in acquiring the Search Dataset within one week. This reply shall contain at least the following information:

(a) An application form with clear and detailed information the undertaking applying for eligibility is to provide in order to enable Alphabet to make the eligibility assessment specified at section 4.2.2, recitals (128) - (132);

(b) A description of the Search Dataset, test data samples and the process and basis under which FRAND prices will be calculated in accordance with sections 4.5.2 and 4.6.6.2.2;

(c) Clear and detailed information regarding:

(1) Process for assessing eligibility

(2) The requirement to submit the Level 1 reasonable assurance report as a condition for being granted initial access to the Search Dataset, and the requirement to submit the Level 2 reasonable assurance report as a condition for maintaining access to the Search Dataset in accordance with the conditions specified in section 4.6.6.5.2; and

(3) Processes for granting access to, ensuring continuity of access to, refusing access to, suspending access to and terminating access to the Search Dataset;

(d) Copies of the template licence agreements in respect of the Search Dataset, Sample A, Sample B and Sample C; and

(e) An e-mail address (to be communicated by the Commission to Alphabet) at which the undertaking applying for eligibility may contact the Commission to provide information or submit questions regarding Alphabet's sharing of the Search Dataset.

(1194) Alphabet must present a draft of this application form (including eligibility questionnaire) to the Commission within 45 days of the Commission's adoption of these measures.

(1195) Alphabet must require the submission of a Level 1 assurance report consisting solely of **a non-confidential version containing the assurance conclusions** of the qualified independent assurance practitioner and confirming that reasonable assurance has been obtained for each of the three assurance objectives defined in section 4.4.4.2.4.1.3.

(1196) Alphabet must require all eligible third-party OSEs to notify Alphabet as soon as they have entered into a contract with an auditor for the purposes of preparing a Level 1 assurance report.

(1197) Alphabet must limit its verification of the Level 1 assurance report to confirming the submission of the report and its formal completeness, meaning that the report is issued by a qualified independent assurance practitioner and contains the assurance conclusions for each of the three assurance objectives defined in section 4.4.4.2.4.1.3 in the prescribed non-confidential format. Alphabet must not reassess the substance or scope of the assurance conclusions expressed by the qualified independent assurance practitioner. Within two weeks of receiving the Level 1 reasonable assurance report (in the case of the Search Dataset and Sample C) and signed licence

agreement (in respect of the Search Dataset and all test data samples), Alphabet must either:

(a) Provide the Search Dataset or test data sample in question to the undertaking applying for eligibility; or

(b) Send the undertaking applying for eligibility a decision rejecting the report in accordance with section 4.6.7.1.2.

(1198) Alphabet must inform the Commission of any request it receives without delay. Alphabet must conclude its eligibility assessment within one week of receipt of a completed due diligence questionnaire and transfer impact assessment (if applicable).

(1199) Alphabet must grant access to the Search Dataset to each eligible third-party OSE within 10 days after it has entered into a licence agreement and accepted the price offer, which is to be finalised within six months of the adoption of these measures in accordance with section 4.6.6.2.2.

4.6.6.1.3. The Commission's assessment

(1200) **First**, the Commission considers that these measures are necessary to ensure that Alphabet provides access to the Search Dataset on FRAND terms. For access to be FRAND, third-party OSEs must have an easy means of contacting Alphabet and enquiring about the process for acquiring Search Dataset and test data samples.

(1201) Transparency is a key element of a FRAND process for data acquisition. A transparent process for Search Dataset acquisition will enable third-party OSEs to fully understand their rights and obligations around access to Search Data. The measures the Commission has specified in this Decision achieve this. They require Alphabet to proactively engage with undertakings applying for eligibility and provide crucial information such as the third-party OSEs' rights and obligations, an application form necessary for assessing eligibility, the template licence agreements, a description of test data samples, the requirements to submit assurance reports, a description of processes for acquiring the Search Dataset as well as processes refusing, suspending and terminating access. This approach received support in the public consultation. For instance, one respondent submitted that transparency from Alphabet on important points would be useful for potential beneficiaries.[1382]

(1202) **Second**, the Commission considers that since submission of a Level 1 reasonable assurance report is a pre-condition for receiving access to the Search Data, Alphabet should be able to receive a non-confidential version containing the assurance conclusions of the independent assurance practitioner in relation to the three assurance objectives defined in section 4.4.4.2.4.1.3. Alphabet's role will therefore be limited to verifying the submission of the report and its formal completeness, without reassessing the substance or scope of the assurance conclusions expressed by the independent assurance practitioner.

(1203) Limiting the report to the non-confidential assurance conclusions is necessary to ensure the protection of the third-party OSE's business secrets and to avoid the exchange of competitively sensitive information. Confidential information that may need to be protected includes confidential aspects of the technical, organisational, and human controls that the third-party OSE has implemented to meet the assurance

[1382] Response to the Public Consultation of [third party]: *"Moreover, even though we don't want excessive documentation, it will be beneficial with a short version / executive summary of the important points and a more detailed version for those interested. An easily accessible helpline / support / helpdesk with a defined SLA would be useful"*, Doc ID […].

objectives, as well as any sensitive financial information relevant to the second assurance objective specified in section 4.4.4.2.4.1.3.

(1204) Such an approach preserves the independence and objectivity of the independent verification mechanism, ensures that verification is strictly confined to the predefined assurance objectives, and prevents disclosure of commercially or competitively sensitive operational or financial information.

(1205) **Third,** to ensure access to the Search Dataset on FRAND terms, it is necessary for Alphabet to submit its application form (containing due diligence questions necessary to assess the matters specified at recitals (128) – (132)) for review within 45 days of the adoption of this Decision. In particular, a review by the Commission will provide a safeguard against Alphabet using its procedural discretion to unfairly, unreasonably or discriminatorily deny access to the Search Dataset, thereby undermining contestability, a risk that was flagged in a number of consultation responses.[1383]

(1206) The Commission therefore concludes that these measures are necessary to enable the sharing of the Search Dataset on FRAND terms.

4.6.6.2. Process for finalising pricing terms

4.6.6.2.1. Introduction

(1207) The Commission intends to set out the process governing the determination and communication of Alphabet's pricing terms following the adoption of these measures. In particular, it specifies the steps by which Alphabet is to identify, calculate and communicate the elements underlying its pricing offers, including the methodology for the allocation of upfront common costs at the beginning of the process.

4.6.6.2.2. Measures

(1208) The Commission specifies the following process for finalising Alphabet's pricing terms and communicating them to third-party OSEs applying for eligibility and, ultimately, to eligible beneficiaries.

(1209) Without prejudice to the obligation outlined in recital (1032), within two months of the adoption of these measures, Alphabet must submit the following elements:

(a) An exhaustive list of cost items and estimates, as well as a description of the nature of the respective items (e.g., WACC, one-off or recurring cost, fixed or variable cost, beneficiary-specific or common, whether the cost items scale with the volume or frequency of data to be shared and to what cost category among the ones listed in (1025) it relates to).

(b) A detailed description of the methodology underlying the pricing calculations it has prepared in accordance with section 4.5.2, including, but not restricted to:

1383 Responses to the public consultation of: [national public authority] *"…the proposed framework appears to leave a significant role to the gatekeeper in assessing eligibility. From an economic standpoint, this raises a clear risk of foreclosure through procedural or informational asymmetries, as access conditions could be used strategically to limit entry. In our view, eligibility criteria should therefore be interpreted broadly and applied under strict supervisory conditions, ensuring that the gatekeeper cannot exercise discretionary control over access. This is a necessary condition for the measure to effectively contribute to market contestability"*; [third party] – *"This framework raises concerns regarding governance and oversight. It assigns Alphabet a central operational role that includes decision-making authority over access…. Although procedural safeguards limit this discretion, Alphabet retains a degree of unilateral decision-making that may create issues in the event of disagreements with third-party OSEs."* Doc ID […].

(1) A description of the methodology used to calculate the WACC, which the reasonable return on the capital employed for the purpose of making the Search Data available cannot exceed.

(2) A description of the methodology used to calculate the margin as used in the pricing scenario laid out in recital (1022).

(3) Any element that remains contingent on the number of eligible beneficiaries, including the allocation of one-off common costs, the applicable formulas, calculation steps and assumptions.[1384]

(1210) In line with recital (1032), Alphabet shall provide confidential and non-confidential versions of the information outlined in recital (1209) to the Commission. Alphabet shall share non-confidential versions of such information, at the appropriate level of granularity to ensure both a sufficient degree of transparency as well as the protection of confidential information, with third-party OSEs applying for eligibility.[1385]

(1211) Within six months of the adoption of these measures, Alphabet shall provide the Commission with, and communicate to all third-party OSEs that have either (i) applied for eligibility and entered into a contract with an auditor for the purposes of preparing a Level 1 assurance report, or (ii) have been assessed as eligible to receive the Search Data following the criteria laid out in section 4.2:

(a) The number of third-party OSEs that have either applied for eligibility and informed Alphabet that they have entered into a contract with an auditor for the purposes of preparing a Level 1 assurance report, or have been assessed as eligible to receive the Search Data; and

(b) The resulting pricing offers, including an allocation of one-off common costs divided equally among third-party OSEs applying for eligibility that have entered into such a contract with an auditor or that have been assessed as eligible to receive the Search Data, following the allocation key laid out in recital (1209)(b)(3).

(1212) The Commission may prolong the six-month period where the proposed methodology in recital (1209) is not deemed appropriate, or where technical or procedural issues have delayed the effective preparation, assessment or implementation of the pricing offer.

(1213) The communication of the pricing offers pursuant to recital (1210) shall be without prejudice to the Commission's assessment of whether Alphabet's methodology complies with these measures and with Article 6(11) of Regulation (EU) 2022/1925.

(1214) If the Commission is of the opinion that Alphabet's calculations are not compliant with these measures or with Article 6(11) of Regulation (EU) 2022/1925, Alphabet shall comply with any directions from the Commission to submit new calculations or other information necessary to calculate FRAND pricing offers within any time limit stipulated by the Commission.

1384 Alphabet shall indicate how the number of eligible beneficiaries, and any subsequent change thereof, will affect the final amount charged to each eligible beneficiary once known.

1385 "Third-party OSEs applying for eligibility" shall have the same meaning as "undertakings applying for eligibility" as defined in recital (128)(a).

4.6.6.2.3. The Commission's assessment

(1215) In its response to the Preliminary Findings, Alphabet raised concerns about the lack of clarity surrounding the process for determining pricing terms. [1386] In particular, Alphabet raised issues about the allocation of the upfront common costs across eligible beneficiaries, and about the uncertainty as to the expected number of the latter.[1387]

(1216) The measures laid down in section 4.6.6.2.2 specify the process by which Alphabet is to identify, calculate and communicate the elements underlying its pricing offers following the adoption of these measures. These measures consider Alphabet's specific concerns on the allocation of costs among eligible beneficiaries in a fast-paced innovation environment. In this sense, the Commission specifies a two-step approach to determining the number of eligible beneficiaries to ensure a proportionate approach that allows for a fair chance to recover the costs incurred in making the Search Data available.

(1217) Furthermore, in view of Alphabet's concerns about a convoluted, complex, and confusing pricing mechanism,[1388] the specific section of the process specified for finalising pricing terms is intended to ensure a sufficient degree of transparency and predictability, for both Alphabet and third-party OSEs applying for eligibility, as regards the pricing terms applicable to them. It is also intended to ensure that upfront common costs are allocated on the basis of a clear and foreseeable methodology at the relevant stage of the access process, avoiding complex ex-post readjustments.

(1218) In addition, specifying such a process is necessary to create appropriate incentives and to reduce the risk that eligible beneficiaries strategically time their request for data sharing.

4.6.6.3. Submission of Level 2 assurance reports to maintain access to the Search Dataset

4.6.6.3.1. Introduction

(1219) As stipulated in section 4.4.4.2.4.1, the Commission has specified in this Decision that Alphabet must require third-party OSEs to submit a Level 2 reasonable assurance report on an annual basis, in order to maintain access to the Search Dataset. The Commission therefore has specified in this Decision a process which is FRAND for the submission of these Level 2 assurance reports and the maintenance of access to the Search Dataset.

4.6.6.3.2. Measures

(1220) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, as a condition for maintaining access to the Search Dataset, Alphabet must require the third-party OSE to submit to Alphabet, on an annual basis, the Level 2 assurance report in accordance with the conditions specified in section 4.4.4.2.4.1:

(a) For the first Level 2 assurance report, within six months of the date the third-party OSE first received access to the Search Dataset;

(b) For all subsequent Level 2 assurance reports, within 12 months of the date on which the previous Level 2 assurance report was submitted.

(1221) In addition, Alphabet must require the third-party OSE to submit to Alphabet, on an *ad hoc* basis, a Level 2 report where it receives a written notification from the

1386 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 531.
1387 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 532.
1388 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 532.

Commission confirming that the Commission is of the opinion that such a report is required in the circumstances. Alphabet must not require any third-party OSE to submit an *ad hoc* Level 2 report unless it has received such written notification from the Commission. Alphabet must also require the third-party OSE to submit this *ad hoc* Level 2 report by a time limit stipulated by the Commission in the Commission's written notification to Alphabet. The decision on whether an *ad hoc* Level 2 report is required, and the time limit for submitting this report, must be solely for the Commission in each instance. If a third-party OSE submits an *ad hoc* Level 2 report concluding reasonable assurance, Alphabet must not require the third-party OSE to submit any further Level 2 report in the period of less than 12 months from the date of submission of the *ad hoc* Level 2 report.

(1222) The Level 2 assurance report must consist solely of a **non-confidential version containing the assurance conclusions** of the qualified independent assurance practitioner confirming that reasonable assurance has been obtained in relation to each of the three assurance objectives defined in section 4.4.4.2.4.1.3.

(1223) Alphabet must limit its verification to confirming the submission of the report and its formal completeness, meaning that the report is issued by a qualified independent assurance practitioner and contains the assurance conclusions for each of the three assurance objectives defined in section 4.4.4.2.4.1.3 in the prescribed non-confidential format. Alphabet must not reassess the substance or scope of the assurance conclusions expressed by the qualified independent assurance practitioner.

(1224) Failure to submit a Level 2 assurance report within the applicable time limits, or failure of the submitted report to confirm that reasonable assurance has been obtained (where the independent assurance practitioner issues a 'limited assurance' conclusion[1389]), must lead to a suspension decision and/or a termination or expedited termination decision in accordance with sections 4.6.7.2.2.1, 4.6.7.3.2 and 4.6.7.4.2. For the avoidance of doubt, this provision must also extend to the submission of *ad hoc* Level 2 reports.

4.6.6.3.3. The Commission's assessment

(1225) As explained in section 4.4.4.2.4.2, the Commission considers that an independent verification mechanism enabling the auditability and verifiability of contractual measures ensuring anonymisation is justified and necessary to ensure that the likelihood of re-identification remains insignificant throughout the duration of access to and processing of the Search Dataset.[1390]

(1226) **First**, because of this, the establishment of a periodic assurance reporting obligation is necessary to ensure the continuous monitoring of the contractual measures ensuring anonymisation over the entire duration of access to the Search Dataset. Without periodic verification, there would be a risk that the effectiveness of the measures implemented by the third-party OSE could deteriorate over time or diverge from the commitments initially undertaken, without timely detection. Requiring an annual assurance report therefore ensures a regular and structured monitoring of compliance with the assurance objectives defined by the Commission while avoiding a disproportionate administrative burden.

1389 As explained in footnote 1179 above, limited assurance provides a lower level of assurance than reasonable assurance, because less extensive procedures are performed and the risk is not reduced to a sufficiently low level to meet reasonable assurance. The practitioner therefore expresses a negative conclusion, typically stating that nothing has come to their attention that causes them to believe the subject matter is materially misstated.

1390 Joint Guidelines, Doc ID […], paragraph 181.

(1227) **Second**, a time limit for submission of the first Level 2 assurance report of six months from the date the third-party OSE first received the Search Dataset is justified. The auditor must conduct this first Level 2 audit based on the first three months of Search Dataset processing and will also require an additional period of up to three months to complete their report and provide non-confidential conclusions. Commencing a Level 2 audit just three months after the initial Level 1 audit is necessary to verify that the third-party OSE is fully complying with the contractual measures ensuring anonymisation from the very beginning of processing. In its revised measures, the Commission proposed that the period between submission of the Level 1 assurance report and the first Level 2 assurance report be reduced to nine months. The Commission has taken Alphabet's comments regarding this period on board and, as requested in Alphabet's response to the Revised Measures, has further reduced the period to six months. Submission of the first Level 2 assurance report just six months after Search Dataset sharing has commenced is necessary to verify that the third-party OSE is complying with the contractual measures justifying the issuing of the Level 1 reasonable assurance report.

(1228) The specified timeframe substantially reduces the period previously envisaged in the Preliminary Findings of 15 months between the Level 1 report and the first Level 2 report. It is further complemented by the provisions around *ad hoc* Level 2 reports, which, taken together, give the Commission and Alphabet substantial tools to ensure third-party OSEs' continued compliance with contractual measures.

(1229) For all subsequent Level 2 assurance reports, a time limit of 12 months from the submission of the previous Level 2 assurance report is justified. The Level 1 and first Level 2 assurance reports will be finalised within just six months of one another. After this initial period of intense audits, Alphabet can satisfy itself that the third-party OSE has put in place the contractual measures and is complying with them in full. A period of 12 months between subsequent Level 2 reports will ensure the continuity of the assurance mechanism based on an annual verification of the effectiveness of the controls in place, while allowing sufficient time for the preparation of the reports. Such an approach will balance the need to ensure the effectiveness of these contractual measures with the need to ensure access on FRAND terms. A more intense audit regime (e.g., Level 2 reports every six months) would create unfair and unreasonable barriers inhibiting third-party OSEs from exercising their rights under Article 6(11) of Regulation (EU) 2022/1925 to access the Search Dataset.

(1230) **Third,** Alphabet's ability, subject to the Commission's prior authorisation, to require submission of an *ad hoc* Level 2 report is necessary to enable the triggering of an audit in case of suspicious activity in between scheduled annual audits, a possibility that Alphabet called for in its response to the Preliminary Findings. The Commission notes a number of concerns raised in response to the public consultation that Alphabet could use procedural rules to unfairly, unreasonably or discriminatorily prevent third-party OSEs from effectively accessing the Search Dataset without greater restrictions on Alphabet's procedural discretion.[1391] In addition, some

[1391] See responses to the public consultation of: [third party] – *"Our core concerns lie with the ambiguity in the procedure for data access. … risks for non-compliance exist in the procedural aspects…. The Commission places limitations on Alphabet in terms of the questions asked, which must not be unduly onerous or require divulging competitively sensitive information…. While prima facie appropriate, these remain high-level principles…."*, Doc ID […]; [national public authority] *"…the proposed framework appears to leave a significant role to the gatekeeper in assessing eligibility. From an economic standpoint, this raises a clear risk of foreclosure through procedural or informational asymmetries, as access conditions could be used strategically to limit entry. In our view, eligibility*

respondents variously called for audit frequency to be decreased,[1392] increased,[1393] or be carried out on a surprise basis.[1394]

(1231) The measure enabling Alphabet, subject to the Commission's prior authorisation in every case, to require submission of an *ad hoc* Level 2 report strikes an appropriate balance between the need to trigger an audit between scheduled annual inspections and the need to constrain Alphabet's discretion. To grant Alphabet discretion to initiate *ad hoc* audits could be used by Alphabet as a procedural means of improperly foreclosing access, thereby breaching the requirement of FRAND access to the Search Dataset.

(1232) Nonetheless, the Commission acknowledges the need for proportionate procedural means to investigate breaches where there are credible suspicions, supported by sound *prima facie* evidence, that third-party OSEs are failing to comply with contractual measures or otherwise misusing the Search Dataset. In this regard, the Commission already has appropriate channels through which to gather such credible evidence. For instance, Alphabet will be able to bring substantiated concerns directly to the Commission's attention. Moreover, concerns may be brought to the Commission's attention by the competent authorities of the Member States (including those responsible for protecting personal data) or by citizens through the Commission's citizen reporting tool for matters concerning Regulation (EU) 2022/1925.[1395] The Commission will also be in a position to fairly and objectively assess the credibility of any suspicions and the *prima facie* soundness of any supporting evidence.

(1233) **Fourth**, for the same reasons explained in recitals (1202) – (1204) in relation to the Level 1 assurance report, Alphabet should only receive a non-confidential version containing the assurance conclusions of the Level 2 assurance report. This is sufficient for Alphabet to satisfy itself that the three assurance objectives defined by the Commission in section 4.4.4.2.4.1.3 have been met. Alphabet's role is therefore limited to verifying the submission of the report and its formal completeness. However, Alphabet cannot be allowed to reassess the substance or scope of the assurance conclusions expressed by the independent assurance practitioner.

---

criteria should therefore be interpreted broadly and applied under strict supervisory conditions, ensuring that the gatekeeper cannot exercise discretionary control over access. This is a necessary condition for the measure to effectively contribute to market contestability", Doc ID […]*;* [third party] – *"This framework raises concerns regarding governance and oversight. It assigns Alphabet a central operational role that includes decision-making authority over access…. Although procedural safeguards limit this discretion, Alphabet retains a degree of unilateral decision-making that may create issues in the event of disagreements with third-party OSEs."* Doc ID […].

1392 See response to the public consultation of [market participant]: *"[We] would encourage the Commission to reconsider the proposed annual Level 2 reasonable assurance cycle. A full annual independent report may be more burdensome than necessary in many cases. A more proportionate model would be a fuller periodic audit, for example every three years, combined with interim attestations and event-driven updates where there is a material change. If the Commission retains an annual framework, it should at minimum ensure that existing reports can be heavily relied upon and that any annual refresh is light-touch"*, Doc ID […].

1393 See response to the public consultation of [third party]: *"Level 2 audits on an annual basis (paragraph 57) leave a window of up to 12 months during which a recipient compromise can remain undetected. … For recipients with access to material volumes of Search Dataset records, audits should be conducted at least every six months, ideally complemented by continuous monitoring (telemetry, anomalous access alerts)"*, Doc ID […].

1394 See response to the public consultation of [third party]: *"I demand … surprise audits…."* (translated from the original French: *«J'exige … des audits surprises»*), Doc ID […].

1395 See: https://digital-markets-act.ec.europa.eu/contact-us-eu-citizen_en

4.6.6.4. Prior notification of a change of control and submission of Level 1 reasonable assurance reports to ensure continuity of access following a change of control of the third-party OSE

4.6.6.4.1. Introduction

(1234) The Commission considers that the measures specified at section 4.4.4.2 must remain enforceable by Alphabet in the event of a change of legal and factual circumstances, including a change of control.[1396] To ensure that those measures remain enforceable, the Commission has specified in this Decision the process and circumstances under which Alphabet must ensure continuity of access to the Search Dataset in the case of a change of control.

4.6.6.4.2. Measures

(1235) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must require written notification from the third-party OSE of any intended change of control over the third-party OSE (including acquisitions of joint control or sole control or changes in the quality of control) within 10 days after it becomes public or at least 30 days prior to the change taking effect, whichever is earlier. Alphabet must transmit the notification to the Commission upon receipt.

(1236) Alphabet must require the notification to identify the natural or legal person(s) acquiring control of the third-party OSE. If this information is not publicly available and is commercially sensitive, Alphabet must require the third-party OSE to notify the Commission directly and share a non-confidential version of the notification with Alphabet.

(1237) Alphabet may conduct a new eligibility assessment in accordance with sections 4.2.2 and 4.6.6.1.2 if it believes based on credible, objective evidence that the change in control could impact on the third-party OSE's eligibility to receive the Search Dataset. Alphabet must conclude this eligibility assessment within one week of receipt of a completed application form (including eligibility questionnaire) and transfer impact assessment, if applicable.

(1238) Subject to this eligibility assessment, following a change of control of the third-party OSE, Alphabet must ensure that the third-party OSE continues to receive access to the Search Dataset immediately after the third-party OSE and the person or persons acquiring control (together the "**merging parties**") submit a new Level 1 reasonable assurance report that takes the change of control into account. Alphabet may only terminate access to the Search Dataset following a change of control of a third-party OSE in accordance with the conditions set out in sections 4.6.7.2.2, 4.6.7.3.2 and 4.6.7.4.2.

4.6.6.4.3. The Commission's assessment

(1239) The measures specified are necessary to ensure that the contractual measures specified at section 4.4.4.2 remain enforceable[1397] while guaranteeing FRAND access to the Search Dataset.

(1240) **First,** the requirement to **notify Alphabet in advance** and **provide a Level 1 reasonable assurance report** to maintain access to the Search Dataset ensures access on FRAND terms. This ensures that third-party OSEs have a clear and transparent process for ensuring access to the Search Dataset in the event they undergo changes of control.

1396 Joint Guidelines, Doc ID […], paragraph 189.

1397 Joint Guidelines, Doc ID […], paragraph 189.

(1241) **Second**, requiring **prior notification** of any intended change of control of a third-party OSE within 10 days after it becomes public or at least 30 days prior to the transaction taking effect (whichever is earlier) is necessary.

(1242) *In the first place*, this requirement will ensure that Alphabet is informed in advance of a potential change of control that might impact on the third-party OSE's ability to meet the assurance objectives specified at section 4.4.4.2.4.1.3. As explained below, a change of control may impact on a third-party OSE's ability to meet those assurance objectives.

(1243) *In the second place,* a notification will put Alphabet on notice that it may prepare to expeditiously terminate if the third-party OSE fails to produce the required Level 1 assurance report before the change of control takes effect. (See further section 4.6.7.4.2 "expedited termination" and the accompanying assessment).

(1244) **Third,** requiring the merging parties to submit **a new Level 1 reasonable assurance report** is necessary to verify that the merging parties meet the assurance objectives specified at section 4.4.4.2.4.1.3. It will thereby ensure the continued effectiveness of all contractual measures specified at section 4.4.4.2.

(1245) *In the first place,* following a change of control, a third-party OSE might be completely absorbed into another business. In those circumstances it will be necessary to verify that the other business does not call into question the implementation of contractual measures specified at section 4.4.4.2 and meets the three assurance objectives.

(1246) *In the second place,* the assurance report in question should be a Level 1 reasonable assurance report rather than a Level 2 reasonable assurance report. The auditor will need to verify the implementation of anonymisation measures by an entity or entities that have not previously received a reasonable assurance report. The auditor should therefore verify the design and suitability of controls to meet the second and third assurance objectives (rather than their operating effectiveness as in a Level 2 situation).

(1247) *In the third place,* the Commission emphasises that, contrary to Alphabet's assertion in its response to the Preliminary Findings, third-party OSEs will be required to notify the change of control and submit the Level 1 reasonable assurance report before the change of control takes effect.

(1248) **Fourth,** the Commission expects third-party OSEs and their potential corporate acquirers to treat the notification of the change of control and submission of a Level 1 report as a condition to continuing to access the Search Dataset. As specified in section 4.6.7.4.2, failure to fulfil either of these conditions may lead to expedited termination and erasure of the Search Dataset from the third-party OSE's servers. Alphabet should make this appropriately clear in its template licence agreements.

4.6.6.5. Submission of Level 2 reasonable assurance reports to ensure continuity of access following the commencement of insolvency proceedings

4.6.6.5.1. Introduction

(1249) The Commission considers that the measures specified at section 4.4.3 (anonymisation) must remain enforceable by Alphabet in the event of a change of legal and factual circumstances, including the initiation of insolvency proceedings against a third-party OSE.[1398] To ensure that those measures remain enforceable, the

[1398] Joint Guidelines, Doc ID […], paragraph 189.

Commission has specified in this Decision the process and circumstances under which Alphabet must ensure continuity of access to the Search Dataset if insolvency proceedings are initiated against the third-party OSE in question.

4.6.6.5.2. Measures

(1250) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must require written notification from the third-party OSE of any insolvency proceedings initiated against it within one week of the initiation of those proceedings. Alphabet must transmit the notification to the Commission upon receipt.

(1251) The notification must identify the jurisdiction and court in which proceedings were brought and briefly describe the circumstances precipitating the proceedings. If this information is not publicly available and is commercially sensitive, Alphabet must require the third-party OSE to notify the Commission directly and share a non-confidential version of the notification with Alphabet.

(1252) Following the initiation of insolvency proceedings, Alphabet must ensure that the third-party OSE continues to receive access to the Search Dataset immediately after the third-party OSE submits a Level 2 reasonable assurance report that takes the insolvency proceedings into account.

(1253) Alphabet may only suspend access to the Search Dataset following initiation of insolvency proceedings in accordance with the conditions set out in section 4.6.7.2.2.

4.6.6.5.3. The Commission's assessment

(1254) The measures specified are necessary to ensure that contractual measures remain enforceable[1399] while guaranteeing FRAND access to the Search Dataset.

(1255) **First,** the requirement to **notify Alphabet in advance** and **provide a Level 2 reasonable assurance** report to maintain access to the Search Dataset ensures that third-party OSEs have a clear and transparent process for ensuring access to the Search Dataset if insolvency proceedings are opened against them.

(1256) **Second**, it is justified for Alphabet to require a third-party OSE to **notify** insolvency proceedings initiated against it within one week of initiation of those proceedings.

(1257) *In the first place*, this requirement will ensure that Alphabet is informed in good time to ensure that it can take appropriate action before the third-party OSE is declared insolvent or substantially restructured. As explained below, imminent insolvency may impact on a third-party OSE's ability to meet the assurance objectives specified in section 4.4.4.2.4.1.3.

(1258) *In the second place,* a notification will put Alphabet on notice that it must prepare to suspend access to the Search Dataset if the third-party OSE fails to produce the required Level 2 assurance report. (See further section 4.6.7.2.2 "suspension of access" and the accompanying assessment).

(1259) **Third,** requiring the third-party OSE to **submit a Level 2 assurance report** is necessary to verify that the third-party OSE continues and can continue to meet the assurance objectives specified at section 4.4.4.2.4.1.3. It will thereby ensure the continued effectiveness of the contractual measures specified at section 4.4.4.2.

(1260) *In the first place,* an undertaking subject to insolvency proceedings (such as those listed in Regulation (EU) 848/2015 or similar proceedings) may be at imminent risk

[1399] Joint Guidelines, Doc ID […], paragraph 189.

of undergoing a change of control, as new investment is needed to keep the undertaking solvent. For the reasons explained above in section 4.6.6.4.3 changes of control can create a risk that the third-party OSE will no longer meet the assurance objectives specified at section 4.4.4.2.4.1.3. An auditor can closely examine a third-party OSE's financial situation and verify whether this risk is credible in the circumstances.

(1261) *In the second place,* an undertaking subject to insolvency proceedings may be at imminent risk of being wound up. In that case, it would cease to exist and would be incapable of remaining the controller of the Search Dataset. It would also be incapable of meeting the assurance objectives specified at section 4.4.4.2.4.1.3. An auditor can verify whether this risk is credible in the circumstances.

(1262) *In the third place,* even if the third-party OSE is not at imminent risk of changing control or being wound up, the situation leading to insolvency proceedings can have a direct impact on third-party OSEs' capacity to maintain contractual measures. Insolvency can result in losses of staff (some of whom may have an important role vis-à-vis contractual measures). It may also lead to a reduction in resources available for protection of data (e.g., failure to upkeep technical infrastructure or train staff).

(1263) **Fourth,** the mere existence of insolvency proceedings against the third-party OSE will not always credibly prove a risk to the contractual measures specified in section 4.4.4.2. Proceedings might be brought even where there is no actual risk of the third-party OSE being unable to pay its debts as they fall due (e.g., because a creditor is acting maliciously). An updated Level 2 assessment is therefore an appropriate control to verify whether the risks identified in the previous recitals are credible. Production of a Level 2 reasonable assurance report is therefore justified to compel Alphabet to ensure continuity of access to the Search Dataset in the event insolvency proceedings are initiated against the third-party OSE.

4.6.7. Processes for refusing, suspending and terminating access to the Search Dataset

4.6.7.1. Refusal decisions

4.6.7.1.1. Introduction

(1264) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. The Commission has specified in this Decision a process for refusing access to the Search Dataset that guarantees access on FRAND terms.

4.6.7.1.2. Measures

(1265) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, if Alphabet decides either:

(a) To deny an undertaking applying for eligibility from accessing the Search Dataset; or

(b) To deny an undertaking applying for eligibility from accessing a test data sample,

it must send the undertaking applying for eligibility a written notification refusing access to the Search Dataset (the "**refusal decision**") by the applicable deadline set out in section 4.6.6.1.2.

(1266) The refusal decision must include at least the following:

(a) **Reasoning:** an explanation of the grounds for the refusal decision;

(b) **Rebutting evidence:** an explanation of the evidence the undertaking applying for eligibility must provide to rebut the refusal decision; and

(c) **Contact:** who the undertaking applying for eligibility can contact and how if it has any questions on the refusal decision.

4.6.7.1.3. The Commission's assessment

(1267) The measures the Commission is considering specifying in respect of refusal decisions are necessary to ensure Alphabet grants access to the Search Dataset on FRAND terms.

(1268) It is fair and reasonable to require Alphabet to inform the undertaking applying for eligibility in question of the reasons for any refusal decision. It is also fair and reasonable to require Alphabet to give undertaking applying for eligibility guidance on who to contact with questions and the evidence the undertaking applying for eligibility may provide to rebut the refusal decision. Rebutting evidence is evidence that may cause Alphabet to revise its refusal decision. This may be the case if there is additional information appropriately addressing the reasons for the refusal decision.

(1269) Transparency is a key element of a fair and effective process. By giving reasons for the refusal decision as well as further guidance, Alphabet will ensure that it handles requests for the Search Dataset and test data samples in a transparent way which is FRAND.

(1270) The Commission therefore concludes that the measures specified are necessary to enable the sharing of the Search Dataset on FRAND terms.

4.6.7.2. Suspension of access

4.6.7.2.1. Introduction

(1271) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. Moreover, the Commission considers that the measures specified at section 4.4.4.2 must remain enforceable by Alphabet in the event of a change of legal and factual circumstances.[1400]

(1272) To ensure that those measures remain enforceable while ensuring access on FRAND terms, the Commission has specified in this Decision the process and circumstances under which Alphabet must suspend access to the Search Dataset.

4.6.7.2.2. Measures

4.6.7.2.2.1. Measures for suspension

(1273) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must suspend an individual third-party OSE's access to the Search Dataset in the following circumstances:

(a) **Failure to submit a Level 2 reasonable assurance report on time:** the third-party OSE does not submit a Level 2 reasonable assurance report within the time limit specified in sections 4.6.6.3.2 (or as specified by the Commission in the case of *ad hoc* audits) or submits a Level 2 report concluding limited assurance; or

(b) **Insolvency:** insolvency proceedings in respect of the third-party OSE are opened.

[1400] Joint Guidelines, Doc ID […], paragraph 189.

(1274) Alphabet must notify the third-party OSE in writing no more than three days after the suspension ("**suspension decision**"). The suspension decision must contain at least the following:

(a) **Reasoning:** a clear and detailed explanation of the grounds for the suspension;

(b) **Effects:** a description of the legal and operational consequences of the suspension;

(c) **Remediation:** a clear and detailed explanation of the evidence the third-party OSE must provide to restore its access to the Search Dataset; and

(d) **Alphabet's obligation to terminate:** the conditions under which Alphabet must terminate access to the Search Dataset specified in section 4.6.7.3.2.

4.6.7.2.2.2. Measures for restoration of access to the Search Dataset

(1275) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must reverse a suspension and restore the third-party OSE's access to the Search Dataset as soon as technically possible once the third-party OSE has remedied the circumstances that triggered the suspension or has otherwise demonstrated that those circumstances no longer apply, in accordance with the conditions set out below.

(1276) In particular, Alphabet must restore access to the Search Dataset in the following circumstances:

(a) **Failure to submit a Level 2 reasonable assurance report on time:** where the third-party OSE submits to Alphabet a Level 2 reasonable assurance report in accordance with section 4.6.6.3.2;

(b) **Submission of a Level 2 assurance report concluding limited assurance:** where the third-party OSE submits to Alphabet a supplemental reasonable assurance report confirming that reasonable assurance has now been obtained for the assurance objectives previously assessed as limited; and

(c) **Insolvency:** where the third-party OSE provides an updated Level 2 reasonable assurance report which takes any relevant changes to the third-party OSE's business that relate to the insolvency proceedings into account.

4.6.7.2.3. The Commission's assessment

(1277) The Commission considers that the conditions governing suspension and restoration of access to the Search Dataset ensure that suspension measures are temporary and limited to justified circumstances while safeguarding the rights of third-party OSEs to restore access once the circumstances that triggered a suspension have been remedied. They thereby ensure that Alphabet shares the Search Dataset with third party OSEs on FRAND terms in line with Article 6(11) of Regulation (EU) 2022/1925.

4.6.7.2.3.1. Suspension measures are limited to justified circumstances

(1278) Alphabet will only be able to suspend access in limited circumstances which are justified to enforce the contractual measures set out in section 4.4.4.2.

(1279) **Failure to submit a Level 2 assurance report on time or submission of a Level 2 report concluding limited assurance:** as explained at section 4.6.6.3.3, submission of a Level 2 reasonable assurance report is necessary to verify the continued effectiveness of contractual measures specified at section 4.4.4.2. If third-party OSEs fail to submit the Level 2 reasonable assurance report within the period specified in section 4.6.6.3.2 (or as specified by the Commission in the case of *ad hoc* audits),

Alphabet cannot ensure that the contractual measures set out in section 4.4.4.2 are complied with and that the necessary protections to achieve anonymisation are in place and effective. It is therefore justified to require Alphabet to suspend access to the Search Dataset in such circumstances.

(1280) **Insolvency:** as explained at section 4.6.6.5.2, initiation of insolvency proceedings against the third-party OSE can indicate that there is a risk to the continued effectiveness of the contractual measures specified at section 4.4.4.2. Until the merging parties produce a Level 2 report taking such proceedings into account, Alphabet cannot ensure that the contractual measures set out in section 4.4.4.2 are complied with and that the necessary protections to achieve anonymisation are in place and effective. To ensure continued effectiveness of these measures, it is therefore appropriate to require Alphabet to suspend access to the Search Dataset.

4.6.7.2.3.2. Third-party OSEs will receive a reasoned decision

(1281) To ensure that any suspension is made in accordance with FRAND procedures, it is appropriate to require Alphabet to notify the third-party OSE in writing.

(1282) The Commission considers that transparency is a key element of a FRAND process. To ensure transparency, it is necessary for Alphabet to clearly set out the reasons for the suspension, the effects, means of remediation and Alphabet's obligation to terminate.

(1283) Moreover, a time limit of three days after the suspension is a fair and reasonable period to require Alphabet to share this reasoned decision. This gives Alphabet sufficient time to prepare the decision after the third-party OSE has failed to meet its obligations.

(1284) It is not necessary to send the reasoned decision in advance of the suspension to ensure access to the Search Dataset on FRAND terms. The third-party OSE will be aware of its obligations in advance as Alphabet will clearly set them out in the template licence agreement.

4.6.7.2.3.3. Restoration of access is guaranteed upon remediation

(1285) To ensure access to the Search Dataset on FRAND terms, Alphabet must restore access immediately once third-party OSEs have remediated the reasons for suspension.

(1286) As explained above, suspension of access is necessary in certain limited circumstances to ensure the effectiveness of the contractual measures specified at section 4.4.4.2. Once these circumstances cease to apply, the suspension is no longer justified. Alphabet would be in breach of its obligations under Article 6(11) of Regulation (EU) 2022/1925 if it continued to deny access to the Search Dataset after the circumstances justifying suspension were remediated.

(1287) Restoration in the circumstances specified in section 4.6.7.2.2.2 is therefore necessary to ensure access on FRAND terms.

4.6.7.2.3.4. Suspension is not limited to administrative circumstances

(1288) A number of responses to the Public Consultation criticised the suspension and termination provisions of the Preliminary Findings, alleging that these remedies were only available in *"administrative"* circumstances such as insolvency.[1401] They

[1401] Responses to the Public Consultation of: [third party] – *"The conditions under which access can be discontinued are currently limited to administrative circumstances – such as insolvency or a change of corporate control – and do not extend to situations where a recipient is found to be combining the*

argued that suspension and termination measures should be extended to situations of substantive breaches of the contractual measures specified at section 4.4.4.2.[1402]

(1289) However, these seem to miss the role of the annual submission of Level 2 reasonable assurance reports. The independent verification mechanism is designed specifically to ensure continued substantive compliance with the contractual measures specified at section 4.4.4.2 and identify and detect breaches. Ongoing verification of compliance is attested by annual resubmission of a reasonable assurance report.

(1290) Failure to submit such a Level 2 reasonable assurance report within the specified time limit or submission of a limited assurance report indicates possible non-compliance with those measures. In those circumstances, Alphabet has the right to suspend access.

(1291) This independent verification mechanism has moreover been strengthened by the addition of the *ad hoc* audit mechanism, which was not foreseen in the Preliminary Findings. This further increases the tools at the Commission and Alphabet's disposal to detect substantive breaches, which may lead to suspension and/or termination of access.

(1292) Accordingly, the suspension grounds specified at section 4.6.7.2.2.1 are sufficiently robust to grant Alphabet the right to suspend access in cases of substantive non-compliance with contractual measures and are not limited to mere administrative circumstances.

4.6.7.3. Termination following suspension

4.6.7.3.1. Introduction

(1293) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset on FRAND terms. Moreover, the Commission considers that the measures specified at section 4.4.4.2 (contractual measures contributing to ensuring anonymisation) must remain enforceable by Alphabet in the event of a change of legal and factual circumstances.[1403]

---

shared data set with external data sources in ways that allow for the reconstruction of individual user profiles", Doc ID […]; [third party] *"The suspension and termination process should include due process and Commission notification, while also covering material misuse and not only formal assurance-report failures, insolvency or change of control. Examples include a verified re-identification attempt, unauthorised onward disclosure, material breach of purpose limitation, failure to maintain required execution-admissibility logs, or critical security-control failure"*, Doc ID […]; [third party] – *"If suspensions are currently limited to specific administrative scenarios, how can the framework address emerging de-anonymization threats, such as third-party data linking? The call for a mechanism to terminate data flows in such cases is compelling, yet the absence of defined triggers or thresholds for intervention introduces uncertainty. Might a more dynamic process—one that balances immediate privacy safeguards with clear, actionable criteria—better ensure both compliance and the protection of European user data"*, Doc ID […]; [third party] *"To maintain the security and confidentiality of European user data, the sharing process must be agile enough to respond to post-sharing inference threats. An economic safeguard must be established to immediately terminate data flows to any third-party recipient found linking the Search Dataset with external sources to reconstruct user profiles, ensuring non-compliant recipients do not retain continuous access"*, Doc ID […]; [third party] – *"Currently, the legal framework appears to permit the suspension of data access only in limited administrative circumstances (e.g., insolvency, change of control). This must be amended to include a clear and immediate right of suspension in cases where there is a demonstrated or reasonably suspected risk of non-compliance with data protection obligations"*, Doc ID […].

1402 Ibid.

1403 Joint Guidelines, Doc ID […], paragraph 189.

(1294) To ensure that those measures remain enforceable while ensuring access on FRAND terms, the Commission has specified in this Decision the process and circumstances under which Alphabet must terminate access to the Search Dataset.

4.6.7.3.2. Measures

(1295) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet must decide to permanently terminate an individual third-party OSE's access to the Search Dataset ("**termination measure**") where a third-party OSE fails to provide the evidence of remediation specified in section 4.6.7.2.2.2 within three months of receiving the suspension decision specified in section 4.6.7.2.2.1.

(1296) Within five working days after it has terminated access, Alphabet must send the third-party OSE a decision which includes at least the following:

(a) **Reasoning:** a detailed explanation of the grounds for the termination decision; and

(b) **Effects:** a detailed explanation of the legal consequences of the termination decision.

(1297) Upon issuing a termination decision, and unless a supervisory authority has opened an investigation or taken investigative steps under Regulation (EU) 2016/679 against the third-party OSE that require the retention of the Search Dataset as evidence, Alphabet must take all necessary contractual measures to ensure:

(a) That the party subject to the termination decision:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset;

and

(b) That any other third party to whom the party subject to the termination decision disclosed (whether intentionally or not) the Search Dataset:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset.

(1298) Alphabet must take all necessary steps to ensure these contractual measures are enforced (including appropriate audit measures to verify erasure, at Alphabet's own expense).

(1299) Alphabet must allow third-party OSEs that have been subject to a termination or expedited termination measure to re-apply for access to the Search Dataset. Alphabet must treat any such subsequent application for the Search Dataset as if it were an application from a new undertaking applying for eligibility. Where a terminated third-party OSE successfully reapplies for the Search Dataset, Alphabet must take into account any past payments of that third-party OSE towards the fixed fee specified in section 4.5.2.

4.6.7.3.3. The Commission's assessment

(1300) **First,** if the third-party OSE has not remedied the circumstances leading to suspension in accordance with section 4.6.7.2.2.2, it is appropriate to require Alphabet to terminate access. This will ensure the continued enforceability of the contractual measures specified at section 4.4.4.2 while ensuring FRAND conditions of access to the Search Dataset.

(1301) **Second,** a time limit of three months from the date of receipt of a suspension decision is FRAND, as it gives the third-party OSE sufficient time to remedy the situation (e.g., by making the necessary changes to its implementation of contractual measures and having an auditor verify those).

(1302) **Third,** regarding the erasure requirement, in response to the Public Consultation, the EDPB welcomed the Commission's preliminary specification that the Search Dataset must not be erased if a data protection supervisory authority has opened an investigation or taken formal investigative steps.[1404] However, it expressed concern that data protection supervisory authorities would only be informed about a suspension or termination decision at the same time as the third-party OSE and invited the Commission to clarify the interplay between these measures.[1405]

(1303) In light of the EDPB's comments, the Commission has specified that, in cases of expedited termination, Alphabet must ensure retention of the Search Dataset for a specified period (see further section 4.6.7.4.2). This period will allow supervisory authorities to decide whether to open an investigation or take investigative steps.

(1304) However, in cases of termination following a suspension, supervisory authorities will already have had three months to decide whether to take investigative steps. It is therefore not necessary to impose a retention obligation in those circumstances. Moreover, to further accommodate the EDPB's concerns and allow supervisory authorities further space to take action, the Commission has lowered the threshold for supervisory authority action from *"formal investigative steps"* to *"investigative steps"*.

(1305) Moreover, the Commission notes that Alphabet may only seek erasure following termination, not suspension. Accordingly, the fact that supervisory authorities will be informed about suspensions at the same time as the third-party OSE will not impact those supervisory authorities' ability to open investigations or take investigative steps as the erasure obligation will only commence three months later.

(1306) Finally, the Commission accepts Alphabet's submission that it should have the right to appoint an auditor, at its own expense, to verify termination.[1406] It has therefore specified this as one of the contractual measures Alphabet must take to ensure erasure.

(1307) **Fourth,** the Commission considers it necessary to specify that terminated third-party OSEs may re-apply for the Search Dataset. To permanently deny access to third-party OSEs that can in future meet eligibility and independent verification requirements would be unfair, unreasonable and discriminatory to such third-party OSEs. Where a third-party OSE makes such a successful reapplication for the Search Dataset, it is also necessary to specify that Alphabet must take into account any past payments of that third-party OSE towards the fixed fee specified in section 4.5.2. For

---

1404 EDPB comments on the proposed measures of 5 May 2026 – *"Paragraph 134 [of the Preliminary Findings] provides for a requirement for Alphabet to take steps to ensure that the Search Dataset is erased and no longer processed, if it issues a termination decision. The EDPB positively notes that an exception to this is provided if a supervisory authority has opened an investigation or taken formal investigative steps requiring the retention of the Search Dataset. However, in accordance with paragraph 143, the supervisory authority would be informed about any suspension or termination at the same time as the third-party OSE in question, thus in practice it will be unlikely that they would have already taken any investigative steps as a result of the notification of suspension by Alphabet. The EDPB also invites the Commission to clarify the interplay between paragraphs 134 and 143"*, Doc ID […].

1405 Ibid.

1406 Alphabet's submission on contractual measures, Doc ID […], page 21.

example, if a terminated third-party OSE has previously paid the fixed fee in full, Alphabet should not seek any further contribution towards that fee. Likewise, Alphabet should deduct any previously paid proportion of the fixed fee from the fixed fee it charges in the event of a successful reapplication. In the event of reapplication, Alphabet should continue to allow the third-party OSE to pay by instalments, as specified in section 4.5.2.

4.6.7.4. Expedited termination

4.6.7.4.1. Introduction

(1308) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. Moreover, the Commission considers that the measures specified at section 4.4.4.2 must remain enforceable by Alphabet in the event of a change of legal and factual circumstances.[1407]

(1309) To ensure that those measures remain enforceable, the Commission considers that there may be exceptional circumstances that require Alphabet to terminate access on an emergency basis without having to comply with the time limits and procedural requirements specified at sections 4.6.7.2.2 and 4.6.7.3.2 (suspension of access and termination following suspension). The measures the Commission has specified in this Decision will ensure that such expedited termination occurs on FRAND terms.

4.6.7.4.2. Measures

(1310) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, Alphabet may decide to issue termination decisions in exceptional circumstances without following the procedures and time limits specified in sections 4.6.7.2.2 and 4.6.7.3.2 ("**expedited termination decisions**").

(1311) Alphabet may only issue an expedited termination decision in the following three circumstances:

(a) **Integrity and confidentiality of the Search Dataset:** where Alphabet becomes aware of substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised.

(b) **Failure to submit a Level 1 reasonable assurance report in the case of a change of control:** the merging parties fail to submit a Level 1 reasonable assurance report before the change of control takes effect;

(c) **Failure to notify a change of control:** the merging parties fail to notify a change of control within 10 days after it becomes public or at least 30 days prior to the change taking effect (whichever is earlier) in accordance with section 4.6.6.4.2.

(1312) The expedited termination decision must include at least the following:

(a) **Reasoning:** a detailed explanation of the grounds for the expedited termination decision including all substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised; and

(b) **Effects:** a detailed explanation of the legal consequences of the termination decision or expedited termination decision.

(1313) To enable supervisory authorities to exercise their functions under Regulation (EU) 2016/679 in the event of expedited termination, Alphabet shall take all necessary contractual measures to ensure that the third-party OSE retains the Search Dataset for

[1407] Joint Guidelines, Doc ID […], paragraph 189.

a period of four weeks following the third-party OSE's receipt of a termination decision.

(1314) Upon the expiry of this four-week period, and unless a supervisory authority has opened an investigation or taken investigative steps under Regulation (EU) 2016/679 against the third-party OSE that require the retention of the Search Dataset as evidence, Alphabet shall take all necessary contractual measures to ensure:

(a) That the party subject to the termination decision:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset;

and

(b) That any other third party to whom the party subject to the termination decision disclosed (whether intentionally or not) the Search Dataset:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset.

(1315) Alphabet must take all necessary steps to ensure these contractual measures are enforced (including appropriate audit measures to verify erasure, at Alphabet's own expense).

4.6.7.4.3. The Commission's assessment

(1316) The Commission considers it appropriate to allow Alphabet to terminate access on an emergency basis in limited cases without following the processes and timelines for suspension and termination specified in sections 4.6.7.2.2 and 4.6.7.3.2. These cases are confined to cases where there is substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised.

(1317) **First,** the Commission's proposed measures in respect of expedited termination are necessary to ensure the continued enforceability of the contractual measures specified in section 4.4.4.2.[1408] If there is substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised, it is highly likely that those measures are no longer effective. Accordingly, it is justified for Alphabet to terminate access on an expedited basis.

(1318) **Second,** the Commission considers it necessary to specify that, in cases of a change of control, failure to submit a Level 1 reasonable assurance report or to notify a change of control should be grounds for expedited termination.

(1319) *Failure to submit a Level 1 reasonable assurance report in the case of a change of control:* as explained in section 4.6.6.4.3, submission of a Level 1 reasonable assurance report is necessary to verify that a change of control has not impacted the continued effectiveness of the contractual measures specified at section 4.4.4.2. Unless the merging parties produce such a report, Alphabet cannot ensure that the contractual measures set out in section 4.4.4.2 are complied with and that the necessary protections to achieve anonymisation are in place and effective. It is therefore justified to require Alphabet to terminate access to the Search Dataset in such circumstances.

(1320) *Failure to notify a change of control:* as explained in section 4.6.6.4.3, prior notification of changes of control is essential to ensure Alphabet is informed of

[1408] Joint Guidelines, Doc ID […], paragraph 189.

changes that might impact the continued effectiveness of contractual measures. If Alphabet is unaware of such changes, it cannot ensure that the contractual measures set out in section 4.4.4.2 are complied with and that the necessary protections to achieve anonymisation are in place and effective. Termination of data access where a third-party OSE fails to notify the intended change of control is justified to ensure it complies with this obligation.

(1321) *Expedited termination as the appropriate remedy for changes of control:* under the Preliminary Findings, the Commission preliminarily specified that Alphabet would have to first suspend access in cases of failure to notify a change of control or submit a Level 1 reasonable assurance report before the change takes effect. Only if the third-party OSE had not remedied this situation within three months of suspension could Alphabet terminate access and seek erasure. However, the Commission has taken note of Alphabet's arguments in its submission on contractual measures that Alphabet should have the right to terminate and seek erasure in such cases without first suspending access.[1409]

(1322) **Third,** expedited termination in these limited emergency circumstances ensures access on FRAND terms. Expedited termination will only be limited to the above cases where urgent action is required. In all other circumstances, third-party OSEs will benefit from the FRAND procedures set out at sections 4.6.7.2.2 and 4.6.7.3.2 (i.e., suspension followed by termination after three months should it fail to remedy the suspension).

(1323) The Commission agrees with Alphabet that this is an appropriate remedy and has therefore specified that Alphabet may terminate access on an expedited basis in such circumstances without first suspending access (thereby removing the requirement to allow the third-party OSE three months to remediate). The Commission accepts that without the power to expeditiously terminate and seek erasure, an unsuitable buyer could gain control of a third-party OSE and access 13 months of the Search Dataset on the third-party OSE's servers despite a possible suspension of access. Such a scenario would allow buyers to circumvent Alphabet's eligibility assessment as well as the independent verification mechanism for three months before Alphabet could terminate access.

4.6.8. Requirement to impose financial penalties in exceptional circumstances

4.6.8.1. Introduction

(1324) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. Moreover, the Commission considers that the measures specified at section 4.4.4.2 must remain enforceable by Alphabet in the event of a change of legal and factual circumstances.[1410]

(1325) To ensure that those measures remain enforceable, the Commission considers that Alphabet must impose financial penalties in exceptional circumstances.

4.6.8.2. Measures

(1326) Alphabet must impose strictly necessary and proportionate financial penalties on a third-party OSE in the following instances:

(a) A third-party OSE fails to notify a change of control in accordance with section 4.6.6.4.2;

1409 Alphabet's submission on contractual measures, Doc ID […], pages 22 – 23.

1410 Joint Guidelines, Doc ID […], paragraph 189.

(b) A third-party OSE fails to notify the commencement of insolvency proceedings against it in accordance with section 4.6.6.5.2;

(c) A third-party OSE fails to notify Alphabet that it has received a limited assurance report;

(d) A third-party OSE fails to comply with the necessary contractual measures imposing erasure of the Search Dataset as per section 4.6.7.3.2; or

(e) A third-party OSE provides materially false information to Alphabet in connection with the independent verification mechanism specified at section 4.4.4.2.4.1.

(1327) Alphabet must not impose financial penalties on third-party OSEs in relation to their processing of the Search Dataset.

4.6.8.3. The Commission's assessment

(1328) The Commission considers that in order to ensure access to the Search Dataset on FRAND terms, Alphabet should only impose financial penalties to the extent necessary to ensure the effective functioning of the independent verification mechanism set out in section 4.4.4.2.4.1 (and which process is detailed in section 4.4.4.2.4.1, 4.6.6.3.2, 4.6.6.4.2 and 4.6.6.5.2), as well as the erasure obligations in section 4.6.7.3.2 and 4.6.7.4.2. To ensure access to the Search Dataset on FRAND terms, Alphabet should refrain from imposing any financial penalties on third-party OSEs in relation to their processing of the Search Dataset.

(1329) **First,** it is essential that the contractual measures the Commission is considering specifying at section 4.4.4.2 (as well as those in respect of erasure at section 4.6.7.3.2) are enforceable.[1411] Enforcement of these measures relies on the independent verification mechanism specified at section 4.4.4.2.4.1, which involves specific transparency obligations on third-party OSEs towards Alphabet. Those transparency obligations notably include submission of expected assurance reports within deadlines or notification to Alphabet of relevant changes in circumstances (such as insolvency proceedings and changes of control) provided in section 4.6.6.

(1330) Failures to behave transparently that seriously undermine these effective functioning of these two procedures (namely the independent verification mechanism and erasure obligations) are:

(a) Where a third-party OSE fails to notify Alphabet of a change of control contrary to section 4.6.6.4.2; or

(b) Where a third-party OSE fails to notify Alphabet of insolvency proceedings initiated against it contrary to section 4.6.6.5.2;

(c) Where a third-party OSE fails to notify Alphabet of receipt of a Level 2 report concluding limited assurance;

(d) Where a third-party OSE fails to comply with contractual measures for erasure of the Search Dataset in accordance with section 4.6.7.3.2 and 4.6.7.4.2; or

(e) Where a third-party OSE provides materially false information to Alphabet in connection with the independent verification mechanism specified at section 4.4.4.2.4.1 (for instance, a forged reasonable assurance report).

(1331) The Commission therefore considers that Alphabet should have an appropriate means of incentivising compliance with these obligations of transparency to ensure

[1411] Joint Guidelines, Doc ID […], paragraph 189

the effective functioning of the independent verification mechanism and erasure obligations (the latter of which are procedural obligations similarly guaranteed by an audit in accordance with section 4.6.7.3.2 and 4.6.7.4.2). Financial penalties in these circumstances create an **incentive for third-party OSEs to inform Alphabet in a timely manner of relevant circumstances so that Alphabet can suspend access in accordance with section 4.6.7.2.2.1.** irrespective of the conclusions of the independent assurance report. Because financial penalties are linked to procedural failures rather than to the substance of the assurance conclusions, third-party OSEs retain a clear incentive to submit the expected assurance report including where it contains a limited assurance conclusion, rather than withholding or delaying its submission in order to avoid the timely adoption of measures or potential sanctions**.**

(1332) **Second**, the Commission considers that Alphabet must not impose financial penalties in relation to the third-party OSE's processing of the Search Dataset.

(1333) As explained in section 4.4.4.2.1.1, the third-party OSEs are separate controllers for the processing of personal data within the Search Dataset. They are therefore responsible for the processing for the processing of personal data of individuals other than end users and for any processing of personal data resulting from a breach of the contractual measures contributing to ensure anonymisation of end users' personal data. Assessing whether a third-party OSE which would have breached the contractual measures has also violated Regulation (EU) 2016/679 falls within the regulatory mandate of the competent supervisory authorities established under Regulation (EU) 2016/679. Limiting financial penalties to objective failures affecting the functioning of the independent verification mechanism therefore ensures that Alphabet does not effectively enforce potential unlawful processing of personal data, which falls within the competence of supervisory authorities under Regulation (EU) 2016/679. **In addition**, Alphabet, as a designated gatekeeper, must ensure access to the Search Dataset on FRAND terms in accordance with Article 6(11) of Regulation (EU) 2022/1925. This obligation requires that the conditions attached to such access, including contractual enforcement mechanisms, do not discourage or prevent eligible third-party OSEs from effectively exercising their right to seek access to the Search Dataset. In particular, the possibility for Alphabet to impose significant financial penalties for alleged breaches of contractual anonymisation measures could expose third-party OSEs to disproportionate financial risks. Such risks could deter potential beneficiaries from seeking access to the Search Dataset in the first place, thereby undermining the practical effectiveness of the FRAND access obligation and the contestability objective pursued by Article 6(11) of Regulation (EU) 2022/1925.

(1334) As explained at recitals (877) and (884), end users retain the rights and remedies under Regulation (EU) 2016/679, including the right to seek judicial remedies and compensation for material or non-material damage suffered as a result of the unlawful processing of their personal data. Since failures to comply with contractual measures ensuring anonymisation of end user personal data may constitute damage to end users (not Alphabet), there is no basis on which to grant Alphabet a right to claim damages for such failures.

(1335) **Third**, in its submission on contractual measures, Alphabet asserted that contractual financial penalties were unenforceable in certain jurisdictions, such as Ireland (which is a Member State of the Union) and the United Kingdom (which is not a Member State of the Union).[1412] However, the fact that some jurisdictions are not suitable for enforcing contractual measures does not mean contractual measures cannot be

[1412] Alphabet's submission on contractual measures, Doc ID […], page 23.

enforced in other jurisdictions (including in a number of EU jurisdictions). It is Alphabet's responsibility to ensure that the financial penalties which are required by the present Decision are enforceable under the laws governing the contract.

4.6.9. Requirement to amend documents and obligation to inform the Commission, data protection supervisory authorities and the public of decisions granting, refusing, suspending, restoring or terminating access

4.6.9.1. Introduction

(1336) Article 6(11) of Regulation (EU) 2022/1925 requires Alphabet to share the Search Dataset with third-party OSEs on FRAND terms. Moreover, Article 8(1) of Regulation (EU) 2022/1925 requires Alphabet to ensure and demonstrate effective compliance with Article 6(11) of Regulation (EU) 2022/1925.

(1337) The Commission considers that transparency is a key element of a FRAND process for sharing the Search Dataset. The Commission therefore has specified in this Decision measures requiring Alphabet to inform the Commission of all decisions refusing, suspending or terminating access to the Search Dataset.

(1338) In doing so, the Commission will also assist Alphabet in complying with its obligation to ensure and demonstrate compliance with Article 6(11) of Regulation (EU) 2022/1925.

(1339) Moreover, the Commission considers that the contractual measures specified in section 4.4.4.2 must remain enforceable.[1413] To ensure this, the Commission considers it necessary in some circumstances for Alphabet to inform the lead supervisory authority and the Commission of Alphabet's decisions refusing, suspending, terminating or restoring access the Search Dataset.

4.6.9.2. Measures

(1340) To meet the requirements of Article 6(11) of Regulation (EU) 2022/1925, the Commission may require Alphabet to amend the documents that it shall produce to implement the present specification within a deadline to be set by the Commission if the Commission finds that these documents do not effectively comply with Article 6(11) of Regulation (EU) 2022/1925 and the measures in the present specification. This includes the documents referred to in recitals (1178), (1193)(a), (1208) and (1211).

(1341) Alphabet must share a copy of any refusal, suspension or termination decision with the Commission at the same time it shares any such refusal, suspension or termination decision with the third-party OSE in question.

(1342) Alphabet must also share a copy of any suspension or termination decision with the lead supervisory authority at the same time it shares any such suspension or termination decision with the third-party OSE in question. Throughout this Decision, *"lead supervisory authority"* means the lead supervisory authority for the processing carried out by the third-party OSE in line with Article 56(1) of Regulation (EU) 2016/679.

(1343) Alphabet must inform the Commission and the lead supervisory authority within five working days of any restoration of access to the Search Dataset following a suspension. It must also provide the reasons for which it has restored access to the Search Dataset.

[1413] Joint Guidelines, Doc ID […], paragraph 189.

(1344) Alphabet must notify the Commission and the lead supervisory authority of the third-party OSE of its intention to issue an expedited termination decision at least three working days before it intends to issue such expedited termination decision to the third-party OSE in question. In its notification, Alphabet must clearly explain the reasons for its expedited termination decision and provide supporting evidence.

(1345) Alphabet must maintain on its website a page listing all third-party OSEs that have received access to the Search Dataset. Alphabet must display on this page a notice in respect of each eligible third-party OSE publicising that Level 1 and Level 2 assurance has been obtained as well as a notice publicising the fact of any termination and expedited termination decisions, as well as a short description of the reasons for such termination or expedited termination decisions. These notices shall not contain any information which is confidential information or business secrets of the third-party OSE.

4.6.9.3. The Commission's assessment

(1346) To ensure compliance with Article 6(11) of Regulation (EU) 2022/1925, the above measures are justified.

(1347) **Requirement to amend documents:** the Commission may require that Alphabet amends the documents it has to produce to comply with this Decision, including the documents referred to in recitals (1178), (1193)(a), (1208) and (1211). This may be necessary to ensure that Alphabet effectively complies with its obligation to share the Search Dataset on FRAND terms and in compliance with the measures set out in this Decision if Alphabet cannot agree with eligible third-party OSEs. The time limits in which Alphabet must implement any required amendments must be at the Commission's discretion in each case to ensure timely and effective implementation of these measures. The Commission may require Alphabet to make amendments to the documents referred to in recitals (1178), (1193)(a), (1208) and (1211) before or after they have been made available to eligible third-party OSEs.

(1348) **Notifying the Commission of decisions refusing, suspending, restoring or terminating access:** to ensure access on FRAND terms, Alphabet should be required to notify the Commission of decisions refusing, suspending, terminating or restoring access to the Search Dataset at the same time as it notifies the third-party OSE in question.

(1349) *In the first place,* these notification requirements are necessary to enable the Commission to monitor Alphabet's ongoing compliance with the requirement to grant the Search Dataset on FRAND terms. They moreover assist Alphabet to comply with its obligation of ensuring and demonstrating compliance with Article 6(11) of Regulation (EU) 2022/1925.

(1350) *In the second place,* it is appropriate that Alphabet notify the Commission at the same time it notifies the third-party OSE in question. This will ensure that the Commission is kept informed on an ongoing basis of any such refusals, suspensions, restorations and terminations and can take appropriate action if these procedures are not being applied on FRAND terms.

(1351) **Notifying the Commission of expedited termination decisions:** it is necessary to require Alphabet to notify the Commission three days in advance of any intended expedited termination decision. A period of three days is reasonable to allow, on one hand, the Commission to give its views on the proposed measure and, on the other, to allow Alphabet to act quickly in cases of urgency. This balances the need to ensure

FRAND access, while preserving the enforceability of the contractual measures specified at section 4.4.4.2.

(1352) **Notifying the lead supervisory authority of decisions suspending or terminating access:** Alphabet should be required to notify the lead supervisory authority of decisions suspending, restoring or terminating access to the Search Dataset at the same time as it notifies the third-party OSE.

(1353) *In the first place,* the notification obligations will contribute to ensuring the continued enforceability of the contractual measures specified at section 4.4.4.2. Many of the criteria specified under the second and third assurance objectives also align with obligations under Regulation (EU) 2016/679.

(1354) *In the second place*, these notifications obligations are also necessary to enable the lead supervisory authority to fulfil its supervisory obligations under Regulation (EU) 2016/679.

(1355) *In the third place,* it is not necessary to notify the lead supervisory of refusal decisions. In the case of refusal, the third-party OSE in question will not be able to process any of the Search Dataset, meaning there will be no data processing for the lead supervisory authority to supervise.

(1356) **Notifying the lead supervisory authority of expedited termination decisions:** it is necessary to require Alphabet to notify the lead supervisory authority three days in advance of any intended expedited termination decision. A period of three days is reasonable to allow the lead supervisory authority to take any steps it needs to discharge its obligations under Regulation (EU) 2016/679.

(1357) **Maintaining a public list of third-party OSEs, Level 1 and Level 2 assurances, termination or expedited termination decisions:** the Commission finally considers it necessary to specify that Alphabet must maintain a public list of third-party OSEs in receipt of the Search Dataset, as well as the fact that Level 1 and Level 2 assurance has been obtained in relation to each such third-party OSE, notices publicising the fact of any termination and expedited termination decisions and a short description of the reasons for such termination or expedited termination decisions.

(1358) *In the first place,* this will grant end users transparency over how their data is being processed. Such transparency has two major benefits. On one hand, it will enable end users to seek remedies under Regulation (EU) 2016/679 in the event of damage suffered as a result of unlawful processing (as explained at recital (877)). On the other hand, it fosters democratic accountability as civil society organisations and the public can scrutinise how the Search Dataset is being processed and shared. The latter is a point that was repeatedly emphasised in response to the Public Consultation.[1414]

[1414] Consultation responses of: [third party] – *"Recommendations … Maintenance of a public list of refused or terminated beneficiaries, redacted as needed."* Doc ID […]*;* [third party] – *"I propose that the eligibility process include transparency mechanisms for civil society and data protection authorities to monitor how beneficiaries use shared data. Regular public reporting on data flows and compliance would strengthen democratic accountability"* (translated from the original French – *« Je propose que le processus d'éligibilité inclue des mécanismes de transparence permettant à la société civile et aux autorités de protection des données de surveiller comment les bénéficiaires utilisent les données partagées. Des rapports publics réguliers sur les flux de données et la conformité renforceraient la responsabilité démocratique »)* Doc ID […]*;* [third party] – *"Recommendation: introduce a publicly available, real-time register of active recipients of the Search Dataset …. This is a basic transparency tool that enables independent scrutiny by researchers, journalists, civil society, and affected citizens,*

(1359) *In the second place,* whistleblowers may come forward if they have evidence that a third-party OSE is violating contractual measures.

(1360) *In the third place,* this public list should contain no more than a list of third-party OSEs receiving the Search Dataset, the fact (but no more details) that a third-party OSE has received Level 1 or Level 2 assurance, and a short description of the fact of and reasons for any termination or expedited termination decisions. To give further information is unnecessary to achieve the aims explained in the previous recitals and could reveal business secrets of the third-party OSEs in question.

5. PROPORTIONALITY

(1361) In its response to the Preliminary Findings, Alphabet argues that the draft measures disregard the principle of proportionality as enshrined in Article 5(4) and Protocol 2 of TEU[1415] and Article 52(1) of the Charter of Fundamental Rights,[1416] in particularly because they interfere with Alphabet's property rights under Article 17 of the Charter of Fundamental Rights.[1417] Alphabet argues that the Commission did not conduct a proportionality assessment,[1418] and that the draft measures rely on the representations of self-interested Search Data recipients rather than balance the interests of all stakeholders.[1419]

(1362) The Commission notes that Alphabet's claims are vague and generic. Alphabet is concerned that the measures can disclose "*the extraordinary value and innovation*" of Google Search, and enable third parties to "*copy*" and "*freeride on*" Alphabet's technology.[1420] Alphabet has not substantiated its claim that the interference of the measures with its property rights is disproportionate. In particular, Alphabet has not explained why the interference with its property rights is of such nature and weight to cast aside, in this particular case, the EU legislator's weighing of the public interests against the private interests of economic operators impacted by that legislation as reflected in the wording of Article 6(11) of Regulation (EU) 2022/1925.

(1363) The Commission also notes that the specified measures adopted under Article 6(11) of Regulation (EU) 2022/1925 in any event comply with Article 17 of the Charter of Fundamental Rights. Article 17 of the Charter of Fundamental rights also lays down that exceptions to the property rights are possible and "*[t]he use of property may be*

---

and is consistent with the public-interest rationale of Article 6(11) DMA." Doc ID […]; and [third party] – *"The Commission should require a public list of approved recipients …"* Doc ID […].

1415 Article 5(4) TEU states: "*Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality*."

1416 Article 52(1) of the Charter of Fundamental Rights states: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

1417 Article 17 of the Charter of Fundamental Rights states: "(*1) Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest. (2) Intellectual property shall be protected*." Alphabet's reply to the Preliminary Findings, Doc ID [...], paragraphs 80-82.

1418 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 83.

1419 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 84-85.

1420 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraph 84(a).

regulated by law in so far as is necessary for the general interest." Article 6(11) of Regulation (EU) 2022/1925 is part of such regulation and balances the property rights of designated gatekeepers with the general interest, namely the promotion of contestability of gatekeeper's position by third-party OSEs thanks to the provision of Search Data. The mere existence of an interference with a property right, even if it was established, would therefore not automatically imply that the measure giving rise to that interference adopted on the basis of Article 6(11) of Regulation (EU) 2022/1925 would be unlawful. As explained in section 3, the Union legislator has already weighed the public interests against the private interests of economic operators impacted by Article 6(11) of Regulation (EU) 2022/1925, including the degree of legal protection of property rights. While the fundamental right to property applies, the text of Article 6(11) of Regulation (EU) 2022/1925 suggests that the EU legislator concluded that certain interferences with the right to property must be accepted to achieve the objectives of that provision. This is even more evident if we take into account Alphabet's proposed revision of Article 6(11) — rejected by the EU legislators — which suggested adding that the search data sharing should be subject to "*proportionate safeguards to protect user safety and privacy, search result manipulation, trade secrets, and intellectual property*".[1421] While the Commission is under a duty to comply with the principle of proportionality and fundamental rights guaranteed under the TEU and the Charter of Fundamental Rights, in the absence of a clear and substantiated argumentation as to why certain measures specifically interfere with Alphabet's property rights, the Commission takes the view that there is no indication that the measures in this Decision disproportionately impact on Alphabet's property rights.

(1364) Notwithstanding, the Commission considers that the measures specified in this Decision are suitable, necessary, and proportionate[1422] to the objective of Article 6(11) of enabling third-party OSEs to optimise their services to contest the gatekeeping OSE.

(1365) **First**, the measures do not require anything beyond the clear scope of Article 6(11) of Regulation (EU) 2022/1925, which requires the sharing of anonymised "*ranking, query, click and view data in relation to free and paid search generated by end users*" on Google Search on FRAND terms. The Union's legislator considered these measures to be suitable, necessary and proportionate to enable third-party OSEs to optimise their OSE services to contest the gatekeeping OSE. This Decision strictly implements this provision by providing guidance on the granularity and conditions of data sharing, but it does not require from Alphabet anything that goes beyond the scope of Article 6(11) of Regulation (EU) 2022/1925.

(1366) **Second**, among all the potential measures which fall within the scope of Article 6(11) of Regulation (EU) 2022/1925, this Decision specifies the measures which are the most suitable to achieve the objective of public interest pursued by Article 6(11) of Regulation (EU) 2022/1925 and are the least restrictive to achieve this aim without imposing an excessive burden on Alphabet.[1423] In particular, the Commission makes the following observations.

(1367) In relation to eligibility, the measures place appropriate limitations on the pool of eligible beneficiaries by enabling Alphabet to screen out undertakings based on

---

1421 Alphabet, "Search Data Disclosure under the DMA" dated 10 November 2021, Doc ID [...], page 24.

1422 See, e.g., the Judgment of 13 November 1990 in Fedesa, Case C-331/88, ECLI:EU:C:1990:391, paragraph 13.

1423 See, e.g., the Judgment of 13 November 1990 in Fedesa, Case C-331/88, ECLI:EU:C:1990:391, paragraph 13

specified eligibility criteria and clarifying that Alphabet can seek an exemption decision where necessary (see section 4.2). Viewed in light of other measures serving complementary aims (e.g., the independent verification mechanism), the eligibility measures strike an appropriate balance between the legitimate aim of screening out unsuitable candidates and the objective of Article 6(11) of Regulation (EU) 2022/1925 to increase contestability in the OSE sector.

(1368) In relation to the data scope and conditions of sharing, the measures do not request Alphabet to share Google Search's "*ranking, query, click and view data*" in all their scope and depth, but they specify a limited sub-set of data based on an objective principle, namely the principle of parity, that is necessary and proportionate for achieving the objective of Article 6(11) of Regulation (EU) 2022/1925.

(a) By following the principle of parity, the measures clarify that Alphabet is not required to provide data beyond what it collects for the purpose of optimising its own OSE. At the same time, this objective criterion allows to focus on the data's suitability for OSE optimisation, as proven by Alphabet's own practices (e.g., requesting only coerced location data).

(b) By considering the views of third-party OSEs, the measures are focused on data which are practically necessary for OSE optimisation. For example, instead of requesting all search results returned to the user in response to a query (counted in millions), the measures request the sharing of only search results which generated an impression (counted in dozens).[1424] At the same time, the views of third parties are subsidiary to the legal analysis and assessed critically (i.e., they come as a third tier of analysis, after the legal analysis and the application of parity principle). Contrary to Alphabet's allegations, the measures do not endorse numerous requests of third parties (e.g., request to share content of advanced search modules[1425], ranked list of most frequently clicked URLs,[1426] user's age metadata[1427], and many more).

(c) The measures also balance the public interests pursued by Article 6(11) of Regulation (EU) 2022/1925 against the interest of Alphabet. In particular, first, the measures do not require sharing certain data points that may potentially be covered by Alphabet's intellectual property (leaving aside the question as to whether that is indeed the case), such as ranking signals [descriprion of Alphabet's internal processes].[1428] Second, the measures limit the data access latency, duration of data access and take into account the technical feasibility of data sharing, ensuring that they are proportionate.[1429] In particular the duration of sharing is capped at five years to avoid the risk of long-term free riding and ensures that incentives for eligible beneficiaries to innovate are maintained. This ensures that the specified measures remain proportionate to the objectives pursued by Article 6(11) of Regulation (EU) 2022/1925. Many limitations to the scope of measures also directly reflect Alphabet's feedback.

1424 [Market participant's] response to RFI 2 of 16 December 2025, Doc ID [...], See the response to the Public Consultation of [third party], Doc [...].

1425 See the following replies to the public consultation: [third party], Doc ID [...]; [third party], Doc ID [...]; [third party], Doc ID [...].

1426 See the following replies to the public consultation: [third party], Doc ID [...]; [third party], Doc ID [...].

1427 See the following replies to the public consultation: [third party], Doc ID [...]; [third parties], Doc ID [...].

1428 See section 4.3.2.4.

1429 See sections 4.3.3.2, 4.3.3.3 and 4.3.3.4.

For example, the exclusion of ad URLs, the data access latency and the duration of data sharing take onboard Alphabet's own proposals.

(1369) In relation to anonymisation, the starting point of the anonymisation measures is that they first need to achieve anonymisation of end user personal data to the legally required standard.[1430] Iin line with Article 6(11) of Regulation (EU) 2022/1925 read in the light of recital 61, "*when selecting among various possible ways of achieving anonymisation of data of end users shared under Article 6(11) DMA, gatekeepers should select the one that preserves the most quality and usefulness of the data for the third party undertaking applying for eligibility to it, while also ensuring that the shared data of end users is anonymised taking into account all the means reasonably likely to be used by the third party undertaking providing online search engine or by another person to identify end users directly or indirectly*".[1431] This ensures that anonymisation measures are proportional, and data quality and usefulness is balanced against the interest of end users to have their personal data protected. As described in section 4.4, the Commission has also carefully considered and assessed all input provided by Alphabet and alternative proposals to ensure that it specifies a proportionate anonymisation method.

(1370) In relation to FRAND pricing, considering the economic and regulatory circumstances and the objectives of Article 6(11) of Regulation EU 2022/1925 as well as the broader goals of fairness and contestability, the Decision weighs in Google Search's gatekeeping position and privileged access to Search Data and eligible beneficiaries' disadvantaged position, to conclude that FRAND pricing terms should allow the latter to obtain effective access to such data to be able to optimise their search services without maintaining or providing Alphabet with an unfair advantage.

(a) Against this background, the Decision considers pricing approaches based both on value and cost methodologies and chooses the most appropriate and proportionate one. The specified cost-based approach, that strictly reflects the incremental costs incurred by Alphabet for the purpose of making the Search Data available, including a reasonable return corresponding to a return on the capital employed for that purpose that shall not exceed Alphabet's WACC, ensures that the specific objectives of Article 6(11) of Regulation (EU) 2022/1925, as well as the broader ones of fairness and contestability, are achieved. In light of the specific circumstances that justified the legislature's regulatory action with the adoption of Regulation (EU) 2022/1925, and in particular the existing barriers to entry and expansion in the market for online search for eligible beneficiaries, and absent an available competitive value based benchmark, a cost-based pricing method is considered to be necessary and appropriate to ensure that access to Search Data is not only made possible, but also effective, and that Alphabet is duly compensated for it without obtaining an unfair advantage. In addition, following Alphabet's requests for increased clarity and transparency in the application of the cost-based methodology, a process for finalising the pricing terms is introduced, including an appropriate way to determine the number of eligible beneficiaries among which the costs are to be allocated.

(b) Moreover, the Decision introduces certain exceptions precisely to safeguards the interests of Alphabet. Provided that eligible beneficiaries do not qualify as

1430 Joint Guidelines, Doc ID [...], paragraphs 179.

1431 Joint Guidelines, Doc ID [...], paragraph 180.

SMEs, where Alphabet could credibly demonstrate that it would not be able to cover the costs of collecting the relevant data, including a reasonable return on capital from its own commercial use of that data, Alphabet may also be entitled to a margin. The same applies when beneficiary operates at a very large scale. At the same time the Decision, again to safeguard the interests of Alphabet, also clarifies that the specified FRAND pricing terms do not apply to other designated gatekeeper under Article 3(4) Regulation (EU) 2022/1925 in relation to the provision of an online search engine core platform service.

(1371) In relation to process, the specified processes strike an appropriate balance between the need to ensure that third-party OSEs can access the Search Dataset on FRAND terms and the need to grant Alphabet suitable procedural tools to enforce contractual measures. They give Alphabet the right to refuse, suspend and terminate access, request *ad hoc* audits and level penalties, subject to necessary and appropriate limitations to protect the rights and interests of third-party OSEs. Many of Alphabet's procedural powers were included at Alphabet's request. For example, in its submission on contractual measures, Alphabet requested powers to order *ad hoc* audits, appoint an auditor at its own expense to verify erasure and expeditiously terminate in the case of failure to notify or provide a Level 1 audit in the case of a change of a change of control.[1432] All of these changes have been included in this Decision.

(1372) While this is not strictly related to the proportionality assessment,[1433] the Commission does not agree with Alphabet that the measures merely replicate the representations of self-interested data recipients and that they do not balance the interests of all stakeholders, including Google Search's users and third-party websites.[1434] For all the measures, the Commission's assessment reflects its legal analysis of the scope of Article 6(11) of Regulation (EU) 2022/1925. Third parties' views have been treated as input to inform the Commission's specification within the clear boundaries of Article 6(11) of Regulation (EU) 2022/1925. The procedure set out in Article 8(2) of Regulation (EU) 2022/1925 for the specification proceedings ensures that all third parties have the opportunity to provide input, in particular through the requirement to organise a public consultation on the draft measures set out in the Preliminary Findings. The Commission has strictly followed this procedure and the specification measures balance the interests of various stakeholders (for instance, the measures do not require sharing the content of advanced search modules or content owned or provided by publishers, but only publicly available URLs to their websites).[1435]

(1373) In conclusion, the Commission considers that Alphabet's arguments on the breach of the principle of proportionality, as well as the arguments on the undue weight given

---

1432 Alphabet's submission on contractual measures, pages 2, 4, 16, 19 and 21.

1433 The case law quoted by Alphabet does not support Alphabet's reading that a balancing of the interests of all stakeholders is an independent element of the proportionality assessment in all cases (Judgment of 13 November 1990, Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, Case C-331/88, para. 13; Judgment of 3 December 2019, Czech Republic, Case C-482/17, para. 79; Judgment of 5 May 1998, United Kingdom of Great Britain and Northern Ireland v Commission of the European Communities, Case C-180/96, para. 96; Judgment of 12 July 2012, Association Kokopelli v Graines Baumaux SAS, Case C-59/11, para. 38).

1434 Alphabet's response to the Preliminary Findings, Doc ID [...], paragraphs 84 and 85.

1435 The measures do not oblige Alphabet to share the content of advanced search modules (e.g., meal recipes, travel itineraries, news, etc.) but merely URLs to which users are directed (e.g., URLs to websites with recipes, travel blog, journals, etc.). This addresses Alphabet's concern that the sharing of content could enable third-party OSEs to simply copy it into their SERPs, violating copyrights of third parties.

to the representations of self-interested data recipients and lack of balancing of interests of all stakeholders must be rejected.

6. CONCLUSION

(1374) For the reasons set out above, the Commission hereby specifies measures pursuant to Article 8(2) of Regulation (EU) 2022/1925 that Alphabet has to implement within the deadlines specified in the Annex to this Decision to effectively comply with the obligations under Article 6(11) of Regulation (EU) 2022/1925 in relation to the sharing of Google Search data.

HAS ADOPTED THIS DECISION:

Article 1

Alphabet shall implement the measures as specified in the Annex to this Decision within the deadlines specified therein pursuant to Article 8(2) of Regulation (EU) 2022/1925.

Article 2

The effectiveness and impact of these measures will be evaluated within two years following the adoption of this Decision, taking into account technological developments.

Article 3

This Decision is addressed to Alphabet Inc., 251 Little Falls Drive, DE 19808, United States, and Google Ireland Ltd, Google Building Gordon House, 4 Barrow St, Grand Canal Dock, Dublin 4, D04 V4X7, Ireland.

Done at Brussels, 16.7.2026

For the Commission

Signed

Henna VIRKKUNEN
Executive Vice-President

DMA.100209 – SP – Alphabet – Article 6(11)

Annex to the Decision of 16 July 2026 – Final Measures

Non-Confidential Version

[This version has been adapted for publication. Only the adopted decision is legally binding.]

TABLE OF CONTENTS

1. Eligibility 1
2. Data scope and conditions of sharing 3
2.1. Data scope 3
2.2. Conditions of data sharing 6
3. Anonymisation 7
3.1. Technical measures 7
3.2. Contractual measures 10
4. FRAND pricing terms 20
5. Process for Search Dataset acquisition and pre-acquisition data testing 24
5.1. Process and practical arrangements for pre-acquisition technical testing 24
5.2. Process for finalising the Search Dataset 25
5.3. Process for finalising the licence agreements for the Search Dataset and the test data samples 26
5.4. Processes for making the Search Dataset available, reviewing eligibility of undertakings applying for eligibility, finalising pricing terms and ensuring continuity of access 26
5.5. Processes for refusing, suspending and terminating access to the Search Dataset 31
5.6. Requirement to impose financial penalties in exceptional circumstances 34
5.7. Requirement to amend documents and obligation to inform the Commission, data protection supervisory authorities and the public of decisions granting, refusing, suspending, restoring or terminating access 34

ANNEX - MEASURES

1. ELIGIBILITY

(1) Alphabet shall engage with any third-party undertaking that expresses interest in applying for eligibility to receive the ranking, query, click and view data in relation to free and paid search generated by end users on its online search engine ("**OSE**") ("**Search Data**") as specified in section 2 to determine whether it is eligible to receive the Search Data following the process specified in section 5.4.1.

(2) Alphabet shall share the Search Data with any third-party undertaking providing OSEs in the EU and in the EEA, ([1]) which meets the definition of an OSE set out in Article 2(5) of Regulation (EU) 2019/1150 and the requirements of the eligibility assessment specified in paragraphs (3) – (9) (an "**eligible third-party OSE**"). Alphabet shall not exclude third-party undertakings, such as undertakings providing AI chatbots with OSE functionalities, to the extent that these undertakings provide an OSE meeting the definition set out in Article 2(5) of Regulation (EU) 2019/1150, even if the OSE is provided as part of a broader service.

(3) Alphabet shall assess:

(a) Whether an undertaking applying for eligibility to receive Search Data (an "**undertaking applying for eligibility**") ([2]) is subject, directly or indirectly, to restrictive measures or other sanctions under Union law; ([3]) and

(b) Whether the undertaking applying for eligibility is subject, directly or indirectly, *de jure* or *de facto*, to the control of a third country that poses a serious and structural non-technical cyber security and/or data protection risk, taking into account the following elements:

(1) The existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(2) Existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(3) The absence of effective judicial remedies, and independent and democratic control mechanisms, that can allow individuals and companies to exercise their rights to the protection of personal data

---

([1]) In the EU as of today and in the EEA following the incorporation of Regulation (EU) 2022/1925 into the Agreement on the European Economic Area.

([2]) In other words, any undertaking that has submitted the application form specified in section 5.4.1.

([3]) "Restrictive measures or other sanctions" should include economic and trade sanctions adopted on the basis of Article 29 of the Treaty on European Union or Article 215 of the Treaty on the Functioning of the European Union, as well as any other applicable law prohibiting, directly or indirectly, the conclusion of contracts for provision of services with that undertaking. For example, these include measures such as those imposed under Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 229, 31.07.2014, pages 1 – 11 or under Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP, OJ L 141, 28.5.2016, pages 79 – 124.

and/or to correct the identified security concerns, including about existing practices referred to in point (2);

(4) Substantiated information about one or more incidents of threat actors controlled from that third country and operating out of the territory of that third country carrying out malicious cyber activities or campaigns, including phishing and theft of personal data; and

(c) Whether the undertaking applying for eligibility is an established company or credible new entrant providing an OSE as a genuine economic activity in the EU. This condition shall be met only if the undertaking applying for eligibility:

(1) Either:

(a) Has provided OSE services in the EU for at least the last two consecutive years at the time of applying for eligibility;

or

(b) Was founded less than two years ago but has received more than EUR 50 million in capital investments;

and

(2) Has had at least 50 000 monthly average users of its OSE services in the EU in the past year.

(4) Alphabet shall conduct this assessment within the time limit specified in section 5.4.1 and in a strictly FRAND and proportionate manner. As far as practicable, Alphabet shall base its assessment on publicly available information. Alphabet may only request strictly necessary additional information from undertakings applying for eligibility to the extent that such information is not publicly available and shall justify why this information is necessary. Alphabet should not require the provision of business secrets of the undertaking applying for eligibility.

(5) To this end, in accordance with section 5.4.1, Alphabet shall prepare a list of fair, reasonable and non-discriminatory ("**FRAND**") and strictly necessary questions for assessing whether an undertaking applying for eligibility meets the eligibility criteria specified in this section. Alphabet may reject an undertaking as ineligible to receive Search Data if: it identifies clear and objective evidence that the undertaking is subject, directly or indirectly, to restrictive measures or other sanctions under Union law; if the undertaking is subject, *de jure* or *de facto,* to the control of a third country that poses a serious and structural non-technical cyber security and/or data protection risk as described in recital (3)(b); or if the undertaking does not meet the above specified quantitative thresholds demonstrating that the undertaking is an established company or credible new entrant providing OSE services as a genuine economic activity in the Union.

(6) As part of its eligibility assessment, Alphabet shall also inquire whether the undertaking applying for eligibility plans to process and maintain the Search Data within the EEA or whether it plans to request access via:

(a) International transfer of the Search Data to a non-EEA country on the basis of an adequacy decision of the Commission; ([4]) or

([4]) Transfers of personal data on the basis of an adequacy decision of the Commission adopted under Article 45 of Regulation (EU) 2016/679 do not require any additional safeguards. Adequacy decisions

(b) International transfers of the Search Data on the basis of one of the relevant transfer tools foreseen in Article 46 of Regulation (EU) 2016/679 towards a non-EEA third country that is not covered by any adequacy decision.

(7) If Alphabet finds that it, as the controller and exporter of the Search Data (as specified in section 3.2.1), is unable to ensure a level of protection essentially equivalent to that guaranteed within the EEA, it shall conclude that the undertaking applying for eligibility is not eligible to access the Search Data.

(8) Irrespective of the eligibility criteria in paragraph (3), where there are credible indications that the communication of the Search Data to such undertakings may undermine the public security of the EU or its Member States, Alphabet may submit a reasoned request asking to be exempted from its obligations under Article 6(11) of Regulation (EU) 2022/1925 with respect to individual undertakings applying for eligibility. The Commission will assess this request pursuant to the exemption procedure set out at Article 10 of Regulation (EU) 2022/1925. This is without prejudice to the Commission's power to initiate the exemption procedure under Article 10 of Regulation (EU) 2022/1925 based on public security grounds on its own initiative.

(9) Neither the eligibility assessment nor the transfer impact assessment (if applicable) nor any potential reasoned request on grounds of public security may replace the condition specified in section 5.4.1 that all undertakings applying for eligibility shall procure a Level 1 reasonable assurance report before Alphabet may grant them access to Search Data. Alphabet shall not seek to substitute its eligibility assessment or transfer impact assessment (if applicable) or potential reasoned request on grounds of public security for the assessment of the independent assurance practitioner specified in section 3.2.4.

2. DATA SCOPE AND CONDITIONS OF SHARING

2.1. Data scope

2.1.1. Query data

(10) Subject to anonymisation requirements, Alphabet shall share with eligible third-party OSEs any query input entered by end users into Google Search on any access point, any modifications made by end users and Alphabet to this initial query, and any other metadata about the user and query, on par with the data collected by Alphabet *for the purpose of optimising its OSE services*.

(11) It follows that Alphabet shall share with eligible third-party OSEs at least the following query data for each access point (e.g., Google Search website and browser omnibox on Chrome and third-party browsers, Google Search widget, Google Search application, Text Search on Android, Google Assistant, Google Lens and Circle to Search):

(a) Query input and modification data:

(1) Query input as entered by end users (the "**initial query**");

---

are made publicly available in the Official Journal and on the Commission's website here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

(2) Query as modified by end users and Alphabet (the "**modified query**"), including the modifications made through query shortcut chips, autocomplete function, entity results, query suggestions, "*see results about*" feature and autocorrect function;

(3) Content of query modifiers;

(4) Identifier of the type of query modification;

(b) Query metadata:

(1) User location;

(2) Query language identifier; and

(3) User device, including mobiles, desktops and tablets.

2.1.2. View data

(12) Subject to anonymisation requirements, Alphabet shall share with eligible third-party OSEs any URLs and the description of visual elements which are displayed on search engine results pages ("**SERPs**"), served to end users in response to their queries and are viewed by them (i.e., they generate an impression), no matter their type, format, structure or tab in which they are included, on par with the data collected by Alphabet *for the purpose of optimising its OSE services*.

(13) It follows that Alphabet shall share with eligible third-party OSEs at least the following view data:

(a) Uniform resource locators ("**URLs**"):

(1) All URLs, regardless of the format of search result (e.g., photos, videos, text);

(2) All URLs, regardless of their structure (e.g., main URLs, associated URLs);

(3) All URLs for organic search results and advanced search results, and placeholders for paid search results, which are displayed in various search modules;

(4) All URLs, including from the following tabs: *"Videos", "Short Videos", "News", "Forums", "Web", "Books"* and "*Images*";

(b) URL identifiers:

(1) Identifier of the type of result format, including text, video and photo;

(2) Identifier of the place of result in the SERP's structure, including main and associated URLs;

(3) Identifier of the type of tab, including, for example *"Web", "Images", "Videos", "News";*

(4) Identifier of the result type, including organic search results, identifier of paid search results, identifier of advanced search results, the latter including the identifier of sub-type, for example*, "Direct Answer", "Knowledge Panel"*;

(c) Description of visual elements:

(1) The fact of displaying and the text included in query input areas in query shortcut chips, entity results, query suggestions, "see results about" feature and similar, which are displayed on SERPs;

(2) The fact of displaying tabs on SERPs and their type; and

(3) The fact of displaying paid search modules and advanced search modules and their types, irrespective of whether such elements are displayed with or without an URL.

2.1.3. Click data

(14) Subject to anonymisation requirements, Alphabet shall share with eligible third-party OSEs any data on user interaction with the SERP as displayed on the user's device, with any visual elements, and any URLs and with the pages linked by these URLs, including the type, order and duration (where relevant) of user actions, or lack thereof, on par with the data collected by Alphabet for the purpose of optimising its OSE services.

(15) It follows that Alphabet shall share with eligible third-party OSEs at least the following click data for each URL or visual element shared pursuant to paragraphs (12) and (13) of these measures (together: "**SERP Element**"):

(a) Order and duration, or the absence of, clicks and clicks back (i.e. clicks indicating the user's return to the SERP following an earlier click) on the SERP Element;

(b) The duration a user viewed the given SERP Element;

(c) The duration, or the absence of, hovering on the SERP Element;

(d) The number, or the absence of, scrolls on the SERP;

(e) The occurrence, or the absence of, swipes within a swipeable SERP Element; and

(f) The occurrence, or the absence of, expansion of a SERP Element.

2.1.4. Ranking data

(16) Subject to anonymisation requirements, for each SERP Element shared pursuant to paragraphs (12) and (13) of these measures, Alphabet shall share with eligible third-party OSEs (i) the SERP Element's absolute, whole page position on the SERP as displayed on the user's device, (ii) the SERP Element's relative ordinal position, in relation to other SERP Elements presented within the same area on the SERP and (iii) any other information on the SERP Element's relative and absolute position, prominence and visibility on the SERP, as displayed on the user's device, on par with the data collected by Alphabet *for the purpose of optimising its OSE services*.

(17) It follows that Alphabet shall share with eligible third-party OSEs at least the following ranking data for each SERP element shared pursuant to paragraphs (12) and (13) of these measures:

(a) Identifier of the absolute, whole page position on the SERP in which the SERP element is displayed (e.g., top area, main column, right side column);

(b) The relative ordinal position of the SERP Element in relation to other SERP Elements displayed in the same SERP area and the identification of all other SERP Elements displayed in the same area; and

(c) Information about the page on which the SERP Element was displayed on the user's device.

2.2. Conditions of data sharing

2.2.1. Invalid traffic

(18) Alphabet shall exclude invalid traffic, i.e., query, view, click and ranking data, that does not originate from a human user or a genuine user interest, from the Search Data shared with eligible third-party OSEs. To exclude invalid traffic, to the extent technically possible, Alphabet shall use the same methods and process it uses itself in its ordinary course of business and shall not give rise to incremental costs attributable to making the data available.

(19) Alphabet shall provide, upon request of eligible third-party OSE information enabling the third party to understand how invalid traffic is excluded and how the exclusion of invalid traffic impacts the dataset, without revealing Alphabet's business secrets.

2.2.2. Latency, batches and time stamps

(20) Alphabet shall share the Search Data with eligible third-party OSEs on par with Alphabet's own latency of accessing the same data for the purpose of optimising its OSE services to the greatest extent that is technically feasible. The sharing of Search Data shall be carried out within a timeframe of no less than 7 days, which reflects *[Business secret - Description of Google's internal systems]*, and some additional days to anonymise and share the data with third-party OSEs. The final latency of Search Data sharing shall be communicated by Alphabet within the time limit specified in section 5 to the Commission, along with a detailed technical description and justification why it is the lowest latency that can be technically achieved (including meaningful and comprehensive information that can be shared and tested with interested third parties without revealing business secrets, and subsequently notified to them).

(21) No matter the final latency, Alphabet shall share the Search Data in daily batches and with daily time stamps.

2.2.3. Method of data sharing

(22) Alphabet shall use the method of sharing that it uses itself internally for sharing the Search Data with eligible third-party OSEs to the greatest extent that is technically feasible, avoiding unnecessary cost or operational friction, and in any case the method of sharing needs to enable effective sharing of Search Data. Alphabet should provide technical support to third-party OSEs accessing the Search Data.

2.2.4. Duration of data sharing

(23) Alphabet shall share the Search Data with eligible third-party OSEs for the period of their choice and up to five years starting from the moment when the Search Data becomes effectively accessible to that specific third party.

(24) Notwithstanding, the Commission reserves the right to reassess and potentially revise the specification of this duration if it determines that the maximum five-year period of Search Data sharing is not sufficient to achieve the objectives set out in Article 6(11) of Regulation (EU) 2022/1925, in accordance with Article 8(9) thereof.

(25) This is without prejudice to Alphabet being obliged to continue offering the Search Data to eligible third-party OSEs for the entire duration of Google Search's designation as a core platform service.

3. ANONYMISATION

(26) The Commission's measures ensure anonymisation of end users' personal data in the Search Data by mitigating the risks of end users' re-identification to an insignificant level through:

(a) **Technical measures**: these measures alter the Search Data and play a prominent role to mitigate the risk of re-identification of end users without substantially degrading the data quality and usefulness (the Search Data after the application of technical measures are referred to as the "**Search Dataset**"). These measures are outlined in section 3.1.

(b) **Contractual measures**: the contractual measures complement the technical measures and further mitigate the residual risks of re-identification of end users. These measures are outlined in section 3.2.

3.1. Technical measures

(27) Alphabet shall share the Search Data daily and at record level in random order. Each input record shall contain a query text with metadata and shall successfully meet the Commission's technical measures to be included in the Search Data. The technical measures consist of the following steps:

(28) **Attribute suppression**. For each record, the following attributes shall be removed ((a) to (k)) and replaced ((l)).

(a) Any end user identifier, i.e., any direct identifier assigned to a user or user session, such as Google account identifiers (e.g., account IDs, usernames), whether the user was signed in, and other associated direct identifiers (e.g., IP addresses, device IDs).

(b) The timestamp of the query. For the avoidance of doubt, the day of the query shall remain available.

(c) Information about the size (height and width) of modules and results.

(d) Information about the distance from each module or result to the top of the SERP.

(e) Information about the share each module or result occupies of the user's viewport.

(f) The access point.

(g) The input format.

(h) Ad URLs. For the avoidance of doubt, the existence of an ad and interaction data related to that ad shall be maintained.

(i) Advanced filters applied to a query.

(j) Results that are Google services which directly include personal information saved in an end user Google account (e.g., Google Maps results with directions to or from home) or the end user's exact location (e.g., Google Maps result

with directions). Alphabet shall submit a list of such result types to the Commission for approval within the time limit specified in section 5.2.

(k) Within sessions in AI Mode, any queries after the initial query (only the initial query of an AI Mode session shall be provided).

(l) Queries in the form of images shall be replaced with a placeholder query. For queries that combine images and text, only the image shall be replaced with a placeholder query. The text shall not be suppressed.

(29) **Allowlist creation:** Alphabet shall generate and update monthly an allowlist of words appearing in search queries from signed-in end users using the past 13 months of EEA search data employing the following procedure:

(a) Alphabet shall split the original query text of each search record into *entities*:

(1) Alphabet shall use personal data detectors to detect addresses, names, phone numbers, location coordinates, IBAN numbers, credit card numbers and other forms of well-known identifiers and resolve them to standard formats.

(2) Alphabet shall split the rest of the query, which has not been detected as personal data, into words based on whitespace, not counting whitespaces between two digits.

For example, the query "*john doe 200 wetstraat brussel 04 12 34 56 78 communications department*" could be split into "john doe" (flagged by the full name detector), "*200 wetstraat brussel*" (flagged by the address detector), "*04 12 34 56 78*" (flagged by a phone number detector), "*communications*", and "*department*" (single words).

(b) For each entity, Alphabet shall count the number of unique signed-in end users who submitted queries containing the entity in the past 13 months in the EEA.

(c) Alphabet shall add an entity to an allowlist for five years if the entity is included in queries issued by more than 50 (w) signed-in end users.

(30) **Length-based thresholds determination**: Based on queries issued in 2025 by both signed-in and signed-out users in the EEA, Alphabet shall compute a length-based character threshold (c) as follows:

(a) For each inferred language in which a query text has been issued, find the value of threshold c so that 95% of unique queries with that inferred language have fewer than c characters.

(31) **Query suppression:** Every day, Alphabet shall apply the following procedure on each search record generated by signed-in and signed-out end users in the past 24 hours in the EEA:

Alphabet shall remove the entire search record from the Search Data if the modified query (see definition in paragraph (11)(a)(2)) does not meet either of two conditions:

(a) **Entity-based threshold**: Alphabet shall split the query text into entities (as described in paragraph (29)) and determine whether all entities are in the allowlist.

(b) **Length-based threshold:** Alphabet shall check whether the query text is shorter than the length threshold of c characters (see paragraph (30)) for the query's associated inferred language.

(32) If the initial query text (see definition in paragraph (11)(a)(1)) is different from the modified query text, Alphabet shall check whether the initial query text meets the two thresholds. If the initial query text does not meet the two thresholds, the initial query text is removed from the search record; otherwise, Alphabet shall add the initial query text as a data field to the corresponding search record.

(33) If the SERP contains query modifier text, Alphabet shall check whether the query modifier text meets the two thresholds. If the query modifier text does not meet the two thresholds, the query modifier text is removed from the search record; otherwise, Alphabet shall add the query modifier text as a data field to the corresponding search record.

(34) **Metadata generalisation:** For queries that pass query suppression, Alphabet shall apply metadata generalisation to each search record. The attribute subject to generalisation is the location. The timeframe for metadata generalisation is that of the data release, i.e. 24 hours.

(35) Alphabet shall share the location data of the end user using the third level of the EU Nomenclature of territorial units for statistics (NUTS 3). ([5])

(36) Alphabet shall check whether at least 1,000 (*r*) signed-in end users have issued a query with the same metadata attribute values for inferred language, location information, and device type. If such condition is not met, Alphabet shall generalise the location to country level. If the r-threshold is still not met, meaning that fewer than 1,000 (*r*) end users submitted queries with the same inferred language and device type in a given country, Alphabet shall remove the query and its corresponding results and metadata from the Search Data.

(37) Within each metadata group, click back time and interaction durations (e.g., hovering and viewing) shall be binned into time intervals expressed in milliseconds and corresponding to the: 20th, 40th, 60th and 80th percentile of their respective duration distributions within the metadata group.

(38) **Mini-sessionisation**: Alphabet shall group records by ordering all records from the same end user chronologically and adding each search record to the previous group if the following conditions are met:

(a) The current search record was generated by one of the following ways:

(1) The user clicked on a query modifier (e.g., "*Did you mean…*" spelling suggestions, autocomplete suggestions, query suggestions, query shortcut chips, entity results, etc.) in the previous record's SERP.

(2) The user entered a new query into the search box on the previous record's SERP, and the previous record's query text is a substring of the current search record's query text.

The maximum length of a mini-session shall be three queries, and a query can only be part of one mini-session (i.e., mini sessions shall not overlap). Clicked modifiers from the last query in a mini-session shall be suppressed.

(39) Alphabet shall tag each search record associated with a group with the same unique random identifier and provide them in chronological order. The location and device metadata of all records in a mini-session are overridden with the location and device metadata of the last record of this mini-session.

([5]) See https://ec.europa.eu/eurostat/web/nuts, last accessed on 29 June 2026.

(40) Alphabet shall include all other data (as defined in section 2.1) unaltered, without applying any additional measures.

(41) Within the time limit set out in section 5.2, Alphabet shall communicate for the Commission's review:

(a) Which personal data detectors and which entity types Alphabet intends to use to recognise entities as part of query suppression, including the parameters such as the likelihood threshold (confidence) of each detector. Alphabet shall explain why it has identified its proposal as the best performing option and why alternatives identified are less suitable.

(b) A list of result types that link to Google services which directly include personal information saved in an end user Google account (e.g., Google Maps results with directions to or from home) or the end user's exact location (e.g., Google Maps result with directions) which shall be suppressed (see paragraph (28)(j)).

(c) The computing resource cost for each of the steps that are part of the technical anonymisation measures, including a detailed explanation of what factors drive the computing cost of each step.

(42) If Alphabet includes any attributes in the dataset that are not explicitly mentioned in section 2.1, it shall determine whether any anonymisation measures are required in relation to that attribute. If so, Alphabet shall propose to the Commission an appropriate anonymisation measure in relation to that attribute, which does not unnecessarily degrade the quality or usefulness of the data. As part of its proposal, Alphabet shall provide a quantitative estimate of the proportion of data altered and suppressed by the proposed measure.

(43) Alphabet shall provide to eligible recipients the following information in relation to the technical anonymisation measures on a quarterly basis:

(a) Which personal data detectors and which entity types Alphabet used to recognise entities as part of query suppression, including the parameters used such as the likelihood threshold (confidence) of each detector and detection performance statistics. Alphabet shall use publicly available personal data detectors (e.g., Google Sensitive Data Protection).

(b) The proportion of unique queries and query volume suppressed and altered for each anonymisation measure and each personal data detector separately, computed over the full quarter.

(44) Alphabet shall update the Commission on relevant technological developments.

3.2. Contractual measures

3.2.1. Roles and responsibilities

(45) Alphabet shall ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, that Alphabet and the third-party OSE are recognised as independent controllers within the meaning of Article 4(7) of Regulation (EU) 2016/679.

(46) Alphabet shall ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, the following allocation of responsibilities:

(a) Alphabet is controller for the processing of end users' personal data carried out to implement the technical measures set out in section 3.1 prior to the sharing or granting access to the Search Dataset;

(b) Alphabet ensures that the sharing or granting access to the Search Dataset is carried out in a secure manner, in accordance with Articles 5(1)(f) and 32 of Regulation (EU) 2016/679 and, where applicable, in compliance with the requirements of Chapter V of that Regulation;

(c) The third-party OSE accessing the Search Dataset is responsible and liable for ensuring the lawful and compliant processing of personal data of individuals other than end users forming part of the Search Dataset under Regulation (EU) 2016/679, including any processing performed by third parties with whom it has contracted to process the Search Dataset on its behalf acting as processors or authorised sub-processors (i.e. subcontractors);

(d) The third-party OSE accessing the Search Dataset is responsible to ensure that any subcontractors involved in the processing of the Search Dataset are contractually bound to implement all relevant contractual measures set out in sections 3.2.2 and 3.2.3, and that contractual arrangements with such subcontractors explicitly provide independent auditor(s) with the right to verify compliance with these contractual measures in line with the measures in section 3.2.4;

(e) The third-party OSE is responsible and liable under Regulation (EU) 2016/679 for any personal data processing resulting from a breach or circumvention of the contractual measures imposed by Alphabet to ensure anonymisation of end users' personal data, including any processing performed by subcontractors, without prejudice to the allocation of responsibility and liability under that Regulation, in particular Article 82 and 83 thereof.

(47) Alphabet shall ensure, through contractual arrangements with third-party OSEs accessing the Search Dataset, that it imposes only the contractual measures complementing the technical measures necessary to ensure anonymisation of the Search Dataset set out in sections 3.2.2, 3.2.3 and 3.2.4, without extending control over the third-party OSE's independent processing activities.

3.2.2. Contractual obligations complementing technical measures to ensure anonymisation from the third-party OSEs 'perspective

(48) **Effective control***:* Alphabet shall require the third-party OSE to maintain the Search Dataset within a processing environment under its effective control. Any processing of the Search Dataset by the third-party OSE's subcontractors shall take place within that processing environment.

(49) **Segregated processing environment:** Alphabet shall require the third-party OSE to process the Search Dataset exclusively within a logically and technically segregated processing environment so as to prevent linking between the Search Dataset and any other auxiliary dataset accessible to the third-party OSE or its subcontractors. The segregated processing environment shall ensure that:

(a) the Search Dataset cannot be queried jointly with auxiliary datasets;

(b) the Search Dataset cannot be copied, merged, synchronised across the third-party OSE's systems with auxiliary datasets;

(c) processing of the Search Dataset by the third-party OSE and its subcontractors is confined to that segregated environment.

(50) **Prohibitions against linking, re-identification and augmentation:** Alphabet shall prohibit the third-party OSE from:

(a) Attempting to link the Search Dataset with any auxiliary datasets at record level;

(b) Attempting to re-identify directly or indirectly end users, including by attempting to determine, learn or annotate which records relate to the same end users (i.e. "**re-sessionisation**") in any way, such as semantic similarity, behavioural fingerprinting or other techniques, beyond any mini-sessions provided as part of the Search Dataset;

(c) Augmenting, enhancing, or processing the Search Dataset in a manner that reverses, weakens, or circumvents applied technical anonymisation measures, including attempts to infer or reconstruct truncated, generalised, or removed attributes.

(51) **Permitted purposes of use***:* Alphabet shall require the third-party OSE to use the Search Dataset solely for the permitted purpose of optimising or improving OSE services, including for instance, search functionalities such as refining retrieval and ranking systems, web crawling and index building, and functionalities such as query analysis, spell-checking, auto-suggestion, auto-completion and, where applicable, for the purpose of optimising and improving grounding systems and search capabilities for AI chatbots insofar as such AI chatbots rely on search retrieval functionalities. ([6])

(52) Alphabet shall prohibit the third-party OSE from using the Search Dataset for other unrelated purposes.

(53) Alphabet may prohibit third-party OSEs from looking up and serving results directly to end users from the Search Dataset.

(54) **Testing safeguard**: where the permitted purpose under paragraph (51) involves the training or fine-tuning of machine learning models, including models supporting ranking, retrieval, or AI chatbot functionalities, Alphabet shall require the third-party OSE to conduct pre-deployment evaluation of the model to ensure that it does not, under reasonably foreseeable inputs, reproduce data from the Search Dataset in a manner exposing end users to risks of re-identification.

(55) **Retention duration***:* Alphabet shall require the third-party OSE to retain the Search Dataset for a period of maximum 13 months.

(56) **Prohibition of onward sharing and disclosure***:* Alphabet shall prohibit the third-party OSE from disclosing, sharing, sublicensing, or otherwise making available any ranking, query, click, or view data forming part of the Search Dataset received pursuant to Article 6(11) of Regulation (EU) 2022/1925 to any third party ([7]).

(57) **Governance and traceability***:* Alphabet shall require the third-party OSE to implement appropriate and proportionate governance and traceability measures enabling verification that the above prohibitions are complied with and that

([6]) For the avoidance of doubt, the permitted purpose only extends to optimising or improving grounding systems and search capabilities for AI chatbots. Training of the general purpose LLM underlying the AI chatbot is excluded from the permitted purpose.

([7]) Third-party online search engines' subcontractors acting as processors or authorised sub-processors are not considered third parties in this context.

processing aligns with the permitted purpose. Such a measure shall include the identification and documentation by the third-party OSE of:

(a) Automated systems and processes accessing the Search Dataset;

(b) Material processing operations involving the Search Dataset;

(c) Models trained or fine-tuned using the Search Dataset that are subject to the testing safeguard provided for in paragraph (54), and results of this testing.

3.2.3. Integrity and confidentiality of the Search Dataset to ensure anonymisation against any other person

(58) Alphabet shall require the third-party OSE to implement and maintain the following organisational, administrative and contractual measures, which constitute essential safeguards necessary to protect the integrity and confidentiality of the Search Dataset, including protection against unauthorised or unlawful access, disclosure, alteration or loss, taking into account the risks arising from its processing and recognised industry standards for protection of sensitive datasets:

(59) **Technical protection of the Search Dataset:** Alphabet shall require the third-party OSE to ensure that the Search Dataset is encrypted when stored in any system or environment under the third-party OSE's control and is encrypted during transmission between systems and environments, using state-of-the-art encryption appropriate for the sensitivity of the Search Dataset and the risks it is intended to mitigate, including unauthorised access resulting from physical loss or theft of storage media, together with appropriate cryptographic key management measures, including secure storage, access restriction, rotation and revocation of encryption keys.

(60) **Access control and access governance measures:** Alphabet shall require the third-party OSE to:

(a) restrict access to the Search Dataset to personnel authorised by the third-party OSE, as well as to systems, strictly necessary for the permitted purposes of use (see paragraph (51))

(b) assign access rights to such authorised personnel in accordance with the principles of least privilege ([8]) and need-to-know ([9]) and to periodically review and revoke access rights to the Search Dataset where such access is no longer necessary;

(c) subject authorised personnel with access to the Search Dataset to phishing-resistant multi-factor authentication;

(d) ensure that authorised personnel with access to the Search Dataset are subject to enforceable confidentiality obligations and receive yearly training regarding access restrictions, secure handling and authorised and prohibited uses of the Search Dataset as well as on applicable governance and traceability documentation obligations.

(61) **Data handling and other protection measures:** Alphabet shall require the third-party OSE to prohibit the copying, downloading or local storage of any data from the

([8]) The least-privilege principle means that personnel, systems, or processes are granted only the minimum level of access permissions necessary to perform their assigned functions.

([9]) The need-to-know principle means that authorised personnel who have been granted access rights may access data only when required for the performance of their assigned tasks.

Search Dataset on any other device, including authorised personnel-managed devices or workstations.

(62) **Physical security measures:** Alphabet shall require the third-party OSE to implement appropriate physical security measures to protect systems and storage media used to store or process the Search Dataset against unauthorised physical access, removal, or tampering.

(63) **Logging, monitoring and accountability measures:** Alphabet shall require the third-party OSE to:

(a) ensure that all access to the Search Dataset is logged, including attribution to individual users or systems, and that such logs are protected against unauthorised access, alteration, or tampering, including through appropriate separation of duties;

(b) to retain access logs for a period of one year, in order to align with the audit requirement set out in section 5.4.5.

(64) **Data life cycle management:** Alphabet shall require the third-party OSE to ensure that the Search Dataset is securely erased or rendered irrecoverable upon expiry of the 13 months retention period in accordance with recognised industry standards.

(65) **System security maintenance and vulnerability management:** Alphabet shall require the third-party OSE to implement and maintain appropriate measures within the segregated processing environment to identify, assess, document, prioritise and timely remediate vulnerabilities and security weaknesses affecting systems, applications, and authorised interfaces used to store, process, or access the Search Dataset, with a view to preventing unauthorised access, disclosure, alteration, or loss of the Search Dataset and maintaining the ongoing confidentiality, integrity, and resilience of the segregated processing environment.

(66) **Data breach reporting:** Alphabet shall require the third-party OSE to implement processes to detect, report, and respond to any actual data breach affecting the integrity or confidentiality of the Search Dataset in accordance with Articles 33 and 34 of Regulation (EU) 2016/679.

(67) Alphabet may provide recommendations to the third-party OSE on the suitable technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset in line with the measures set out in this section.

3.2.4. Independent verification mechanism to ensure the auditability and verifiability of anonymisation over time

(68) Alphabet shall require third-party OSE seeking access to the Search Dataset to provide an independent reasonable assurance report based on the audit scope and assurance objectives defined throughout this section.

3.2.4.1. General requirements for independent reasonable assurance report

(69) Alphabet shall require a third-party OSE seeking access to the Search Dataset, as a condition for obtaining and maintaining such access, to provide Alphabet with an independent assurance report providing reasonable assurance on the suitability and effectiveness of the controls implemented by the third-party OSE (also referred below as "**reasonable assurance report**") ([10]) to demonstrate compliance with the

([10]) *International Framework for Assurance Engagements* issued by the International Auditing and Assurance Standards Board (IESBA), "Reasonable assurance engagements and limited assurance

assurance objectives defined by the Commission in section 3.2.4.3 below (first, second and third assurance objectives).

(70) The assurance reports shall be prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, and shall cover the organisational, technical, and governance measures implemented by the third-party OSE in relation to the access, storage, processing, use, and protection of the Search Dataset received pursuant to Article 6(11) of Regulation (EU) 2022/1925, within the scope and in accordance with the three assurance objectives defined by the Commission in this section.

(71) The assurance reports shall be issued by an independent assurance practitioner and shall include a written signed declaration confirming the practitioner's independence, qualifications, experience, and compliance with the ethical requirements applicable under ISAE 3000 or, where applicable, under an equivalent assurance framework, including requirements equivalent to those set out in the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA).

(72) As a condition for being granted initial access to the Search Dataset, Alphabet shall require the third-party OSE to submit to Alphabet, in accordance with the conditions set out in section 5.4.1, a **Level 1 assurance report** prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, providing **reasonable assurance** on the first Commission-defined assurance objective as well as **on the design and suitability of the controls** put in place to meet the second and third Commission-defined assurance objectives.

(73) As a condition for maintaining access to the Search Dataset, Alphabet shall require the third-party OSE to submit to Alphabet, on an annual basis and in accordance with the conditions set out in section 5.4.3, a **Level 2 assurance report** prepared in accordance with ISAE 3000 or an equivalent internationally recognised assurance framework, providing **reasonable assurance** on the first Commission-defined assurance objective as well as **on the operating effectiveness of those controls** and covering the Commission-defined assurance objectives. For the purposes of the Level 2 assurance report, the independent assurance practitioner shall assess the operating effectiveness of the controls based on audit testing and sampling drawn from a continuous operating period of not less than 12 months within the reporting period, during which the controls were implemented and operational, with the

---

engagement", paragraphs 14-16: available here: https://ifacweb.blob.core.windows.net/publicfiles/2024-08/IAASB-2023-2024-Handbook-Volume-4.pdf#page=46

A **reasonable assurance engagement** is defined as an assurance engagement in which the practitioner reduces assurance engagement risk to an acceptably low level in the circumstances of the engagement as the basis for a positive form of expression of the practitioner's conclusion. In practice, **reasonable assurance** therefore refers to a **high, but not absolute, level of assurance**, obtained by reducing engagement risk to an acceptably low level. This allows the practitioner to express a **positive conclusion** regarding whether the subject matter meets the applicable criteria.

By contrast, a **limited assurance engagement** is defined as an assurance engagement in which the practitioner reduces assurance engagement risk to a level that is acceptable in the circumstances of the engagement but where that risk is greater than for a reasonable assurance engagement, as the basis for a negative form of expression of the practitioner's conclusion. Accordingly, **limited assurance** provides a **lower level of assurance than reasonable assurance**, because less extensive procedures are performed and the risk is not reduced to a sufficiently low level to meet reasonable assurance. The practitioner therefore expresses a negative conclusion, typically stating that nothing has come to their attention that causes them to believe the subject matter is materially misstated.

exception of the first Level 2 assurance report which must be submitted on audit testing and sampling drawn from a continuous operating period of 3 months.

(74) Where the third-party OSE has obtained existing independent assurance reports, certifications, or audit reports (for example, ISAE 3000, ISAE 3402, SOC 2, ISO/IEC 27001, or equivalent), the auditor conducting the Level 1 or Level 2 engagement shall take such reports into account, in whole or in part, when performing the engagement. In doing so, the auditor shall ensure that:

(a) The scope, period, and assurance criteria of the existing reports demonstrably cover the Commission-defined assurance objectives;

(b) The reports cover the systems, environments, and organisational units within scope pursuant to section 3.2.4.2; and

(c) Any material gaps between the existing reports and the applicable assurance objectives are addressed through a targeted supplemental reasonable assurance engagement ([11]).

(75) The measures Alphabet shall take regarding the submission of Level 1 and Level 2 assurance reports, the formal evaluation of those reports, and any resulting actions (including suspension of access, restoration of access or termination) in cases where the third-party OSE fails to provide a reasonable assurance report are set out in section 5.

3.2.4.2. Audit scope

(76) **Data scope***:* the scope of the assurance engagement shall be limited exclusively to the click, query, ranking and view data made available to the third-party OSE pursuant to Article 6(11) of Regulation (EU) 2022/1925 (the "**Search Dataset**"), including any datasets, models or outputs directly derived from such the Search Dataset within the segregated processing environment. The assurance engagement shall assess the implementation and effectiveness of measures protecting the Search Dataset, as required under the contractual obligations in sections 3.2.2 and 3.2.3.

(77) **Organisational scope**: the assurance engagement shall cover only those parts of the third-party OSE's organisation that process, access, store, or otherwise handle the Search Dataset, including:

(a) the relevant business units, teams, and personnel with authorised access;

(b) internal governance, compliance, and oversight functions responsible for ensuring compliance with contractual obligations relating to the use, security, and anonymisation of the Search Dataset;

(c) any processors or internal service providers involved in processing the Search Dataset on behalf of the third-party OSE; and

(d) where necessary to achieve the assurance objectives organisational units and personnel responsible for planning, budgeting, and allocating resources or financial commitments directly associated with the development, improvement, or optimisation of the search engine using the Search Dataset.

([11]) In this context, the targeted supplemental reasonable assurance engagement means a reasonable assurance engagement, performed in accordance with applicable international assurance standards, that is limited in scope to specific controls or systems and carried out for the purpose of addressing material gaps between existing assurance reports, certifications, or audit reports and the assurance objectives defined by the Commission.

(78) Organisational units, systems, or personnel that do not have physical, logical, or administrative access to the Search Dataset or whose financial or resource activities are unrelated to the Search Dataset processing shall be excluded, provided that effective segregation is demonstrably implemented and maintained.

(79) **Technical scope:** the assurance engagement shall cover all technical systems, environments, and controls used to:

(a) access or receive the Search Dataset from Alphabet;

(b) store, process, or otherwise handle the Search Dataset, including backup and recovery systems;

(c) analyse the Search Dataset or generate outputs, models, or derived datasets based on the Search Dataset; and

(d) manage, monitor, and log access to the Search Dataset.

(80) This includes, where applicable, cloud-based and on-premises environments, development, testing, and production systems in which the Search Dataset is present, as well as identity and access management systems, network security controls, and monitoring and logging systems relevant to the enforcement of contractual obligations for integrity, confidentiality, and continued anonymisation of the Search Dataset.

(81) Where reliance is placed on existing assurance reports, the assurance engagement may be limited to a mapping and gap assessment demonstrating how the controls and findings in such reports apply to the Search Dataset and any directly derived datasets or models.

3.2.4.3. Assurance objectives

(82) The assurance engagement shall evaluate whether the third-party OSE satisfies the conditions applicable to the provision and use of the Search Dataset. In particular, the auditor shall assess whether:

(a) the third-party OSE has established credible and documented plans demonstrating that the Search Dataset will be used for the genuine development, improvement, or optimisation of its own OSE services (First assurance objective);

(b) the third-party OSE has implemented effective technical, organisational, and contractual measures to ensure that the Search Dataset is processed in compliance with the contractual obligations set out in section 3.2.2 (Second assurance objective); and

(c) the third-party OSE has implemented effective technical, organisational, and contractual measures to protect the integrity and confidentiality of the Search Dataset in compliance with the contractual obligations set out in 3.2.3 (Third assurance objective).

(83) **First**, the auditor shall verify whether the third-party OSE has established and maintains credible and documented plans, governance arrangements, and resource commitments demonstrating that the Search Dataset accessed pursuant to Article 6(11) of Regulation (EU) 2022/1925 will be and/or is used for the genuine development, improvement, or optimisation of its own OSE services, in line with the permitted purposes of use and without undermining anonymisation measures. This objective is assessed by verifying:

(a) documented investment planning and financial commitments, including the existence of formal investment plans, budgets, or strategic programmes approved by senior management that allocate dedicated resources to the development or improvement of the third-party OSE's own search technology, and that clearly identify how, and for which development activities, the Search Dataset accessed pursuant to Article 6(11) of Regulation (EU) 2022/1925 is intended to be used for optimising OSE services.

(b) credibility of investment plans, including evidence that planned investments, budgets, or strategic programmes are genuine and realistic in scale, timeframe, and scope relative to the stated development objectives.

(c) adequacy of resourcing for implementing or preserving anonymisation-of the Search Dataset.

(d) that the third-party OSE only serves search results generated by its own search algorithms and technologies and does not merely copy search results directly from the Search Dataset.

(84) **Second**, the auditor shall verify that the third-party OSE has implemented effective measures contributing to ensuring anonymisation of the Search Dataset over time. This objective is assessed by verifying the suitability and effectiveness of technical, organisational, and human controls in the following areas:

(a) Ensuring that the Search Dataset is maintained within a processing environment under the effective control of the third-party OSE and that any processing of the Search Dataset by the third-party OSE or its subcontractors take place only within that processing environment.

(b) Ensuring that the Search Dataset is maintained exclusively within a logically and technically segregated processing environment and that processing of the Search Dataset by the third-party OSE and its subcontractors is confined to that environment, such that the Search Dataset cannot be linked with any auxiliary dataset accessible to the third-party OSE or its subcontractors. In particular, technical and organisational controls must effectively prevent the Search Dataset from:

(1) being queried jointly with auxiliary datasets;

(2) being copied, merged, synchronised across the third party OSE's systems with auxiliary datasets;

(c) Ensuring that the Search Dataset is used solely for the permitted purposes of use of optimising or improving OSE services as specified in paragraph (51) and is not processed for unrelated purposes.

(d) Preventing, detecting and responding to any attempts, whether intentional or incidental, to:

(1) link the Search Dataset with auxiliary datasets at record level;

(2) re-identify end users, including by attempting to determine, learn or annotate which records relate to the same end user (i.e. "re-sessionisation") in any way, such as semantic similarity, behavioural fingerprinting or other techniques beyond any mini-sessionisation provided as part of the Search Dataset; or

(3) augment, enhance, or process the Search Dataset in a manner that reverses, weakens, or circumvents applied technical anonymisation measures, including attempts to infer or reconstruct generalised, truncated, or removed attributes. ([12])

(e) Ensuring that the third-party OSE conducts and documents pre-deployment evaluation of the machine learning models, including models supporting ranking, retrieval, or AI chatbot functionalities that were trained with the Search Dataset model to verify that it does not, under reasonably foreseeable inputs, reproduce data from the Search Dataset in a manner exposing end users to risks of re-identification.

(f) Preventing, detecting and responding to any unauthorised disclosure, sharing, sublicensing, or other making available of the Search Dataset to third parties.

(g) Maintains accurate and up-to-date documentation of automated systems and processes accessing the Search Dataset, material processing operations involving the Search Dataset and models trained or fine-tuned using the Search Dataset that are subject to the testing safeguard provided for in paragraph (54) and testing results in a manner that enables verification that the processing complies with the contractual prohibitions and remains aligned with the permitted uses.

(85) **Third**, the auditor shall verify that the measures implemented by the third-party OSE are designed to protect the integrity and confidentiality of the Search Dataset against unauthorised access, disclosure, alteration, or loss, including in the event of internal misuse or external compromise. This objective is assessed by verifying the suitability and effectiveness of technical, organisational, and human controls in the following areas:

(a) Ensuring that the Search Dataset is encrypted when stored or transmitted between systems or environments under the third-party OSE's control, using state-of-the-art encryption appropriate to the sensitivity of the data and the risks it is intended to mitigate, including unauthorised access resulting from physical loss or theft of storage media, and that appropriate cryptographic key management measures are implemented, including secure storage, access restriction, rotation and revocation of encryption keys.

(b) Restricting access to the Search Dataset to authorised personnel and systems strictly necessary for the permitted purpose and assigning access rights in accordance with the principles of least privilege and need-to-know, with periodic review and revocation of access rights where access is no longer necessary.

(c) Requiring authorised personnel with access to use phishing-resistant multi-factor authentication.

(d) Ensuring that authorised personnel with access to the Search Dataset are subject to enforceable confidentiality obligations and receive yearly training regarding access restrictions, secure handling requirements, authorised and prohibited uses of the Search Dataset, and applicable governance and traceability obligations.

([12]) Data enrichment is permitted if it is limited to transformations that do not increase the risk of re-identification.

(e) Prohibiting the copying, downloading, or local storage of the Search Dataset on any other device, including personnel-managed devices or workstations.

(f) Implementing appropriate physical security measures to protect systems and storage media used to store or process the Search Dataset against unauthorised physical access, removal, or tampering.

(g) Ensuring that all access to the Search Dataset is logged and monitored, including attribution to individual users or systems, and that such logs are protected against unauthorised access, alteration, or tampering, including through appropriate separation of duties, and retained for a period of one year enabling independent audit.

(h) Ensuring that appropriate measures are implemented and maintained to identify, assess, document, prioritise and timely remediate vulnerabilities and security weaknesses affecting systems, applications and authorised interfaces used to store, process or access the Search Dataset, with a view to preventing unauthorised access, disclosure, alteration or loss of the Search Dataset and maintaining the confidentiality, integrity and resilience of the segregated processing environment.

(i) Ensuring that the Search Dataset is securely erased or rendered irrecoverable upon expiry of the 13 months applicable retention period, in accordance with recognised industry standards.

(j) Ensuring that robust, documented and auditable processes are implemented to detect, assess, report, and respond to actual or suspected data breaches affecting the integrity or confidentiality of the Search Dataset in accordance with Articles 33 and 34 of Regulation (EU) 2016/679. The auditor shall verify that:

(1) Appropriate policies, procedures, and controls are established and implemented to ensure the timely detection, escalation, assessment, notification and where required, communication of data breaches within the applicable deadlines;

(2) All data breaches are systematically recorded in a breach register, including the facts relating to the breach, its effects, and the remedial actions taken;

(3) Sufficient and traceable evidence (including logs, incident reports, communications, and post-incident reviews) is retained to allow *ex post* verification of compliance.

(86) The auditor can take into account Alphabet's recommendations regarding the technical, organisational and human controls to protect the integrity and confidentiality of the Search Dataset when assessing the suitability and effectiveness of the third-party OSE's controls.

4. FRAND PRICING TERMS

(87) Alphabet shall provide the Search Data to eligible beneficiaries against a fair, reasonable, and non-discriminatory compensation that strictly reflects the incremental costs incurred by Alphabet for the purpose of making such Search Data available plus a reasonable return, corresponding to a return on the capital employed

for that purpose, that shall not exceed Alphabet's weighted average cost of capital ("**WACC**").

(88) By way of exception to paragraph (87), Alphabet shall not be constrained to a compensation strictly reflecting incremental costs incurred for the purpose of making such Search Data available and a reasonable return corresponding to a return on the capital employed for the purpose of the provision of access to Search Data that shall not exceed Alphabet's WACC in the event that, (i) Alphabet demonstrates that it would not be able to cover the costs efficiently incurred for collecting the relevant data, including a reasonable return, from its own commercial use of that data, ([13]) or (ii) when an eligible beneficiary operates at a very large scale. ([14]) In these circumstances, Alphabet shall also be entitled to a margin, which cannot exceed the operating margin, in percentage terms, of Alphabet's Google Search business, and provided that any resulting terms, taking into account the relevant circumstances, remain FRAND within the meaning of Article 6(11) of Regulation (EU) 2022/1925.

(89) Notwithstanding paragraph (88), micro, small and medium-sized enterprises (SMEs), as defined by Article 2 of the Annex to Commission Recommendation 2003/361/EC, ([15]) shall be exempted from paying more than the incremental costs incurred by Alphabet for the purpose of making Search Data available and a reasonable return on the capital employed for that purpose that shall not exceed Alphabet's WACC, irrespective of whether Alphabet demonstrates its inability to cover the efficiently incurred costs as set out under paragraph (88) above.

(90) Whether Alphabet negotiates the compensation with certain eligible beneficiaries in line with paragraph (100) shall be without prejudice to the application of the cost-based calculation methodology in line with paragraph (87), and cost-allocation principles, for all other eligible beneficiaries. In particular, the fact that Alphabet negotiates the compensation with certain eligible beneficiaries in line with paragraph (100) shall not affect the cost base or the pro rata allocation parameters applicable to other eligible beneficiaries, which shall be calculated as if all eligible beneficiaries were subject to the incremental cost-based methodology specifying a compensation as laid out in paragraph (87).

(91) Cost items that qualify as strictly incremental and incurred by Alphabet for the purpose of making the Search Data available to eligible beneficiaries shall include all costs (irrespective of whether they could be otherwise categorised as fixed or variable costs) pertaining to the following activities ([16]):

(a) Preparing and formatting the dataset with a view to making the Search Data available, that is, all costs directly attributable to the data-sharing-specific further processing of data already stored in Alphabet's databases, in the

---

([13]) The revenue from Alphabet's commercial use of the data should at least include Google Search revenue, which is defined in this context as any revenue directly or indirectly attributable to the provision, operation, or monetisation of the Google Search service, including revenues generated through search advertising, intermediation of search-related traffic, and any other commercial activities deriving value from search queries or search-related user interactions.

([14]) Very large scale is being defined in this context as having more than 45 million monthly active end users established or located in the Union and an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years, or an average market capitalisation or equivalent fair market value amounted to at least EUR 75 billion in the last financial year, calculated in line with Article 3(2)(a) and (b) of Regulation (EU) 2022/1925.

([15]) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Official Journal L 124, 20/05/2003 P. 0036 - 004

([16]) Including common costs arising from making the data available.

absence of the data-sharing provision, including any data-format adaptations, sub-setting or transformations performed with the objective of protecting data subjects, such as anonymisation.

(b) Storage, that is, storage costs linked to making the Search Data available to eligible beneficiaries. Storage costs should only be part of the cost calculation to the extent that the storage environment is used for storing data with a view to making it available to eligible beneficiaries.

(c) Dissemination, that is, costs incurred in the process of electronically transmitting data to eligible beneficiaries, including technical onboarding costs and the costs of operating the Search Data access tools.

(92) The above incremental costs can be classified along two dimensions depending on (i) whether they are recurrent or one-off and (ii) whether they are beneficiary-specific or common across beneficiaries. This results in four categories of incremental costs: one-off beneficiary-specific costs, such as beneficiary-specific technical onboarding costs; one-off common costs, such as the development and set-up of the data sharing service; recurrent beneficiary-specific costs, such as transmission costs attributable to a specific beneficiary; and recurrent common costs, such as overhead costs common across beneficiaries.

(93) The reasonable return on the capital employed for the purpose of making the Search Data available, that Alphabet may also include as part of the compensation, may not exceed Alphabet's WACC. Capital employed for the purpose of making the Search Data available shall be understood as the incremental capital strictly necessary for making the Search Data available.

(94) Alphabet shall implement a per-beneficiary payment scheme which contains a fixed and variable component (two-part tariff). The fixed component ("**fixed fee**") shall be determined independently of the duration of access, the volume of data consumed and the timing at which the beneficiary obtains access. The fixed fee covers, in addition to one-off beneficiary-specific costs, a share of the one-off common costs, which shall be allocated on the basis of the allocation key referred to in paragraph (97)(a). Alphabet shall offer beneficiaries the possibility to pay their fixed fee over the duration of the contract, without prejudice to Alphabet's right to obtain full payment of the fixed fee should a beneficiary decide to discontinue its access to the Search Data before the last invoicing period. ([17]) The variable component covers the beneficiary-specific recurrent costs of making the data available in a given year, as well as the recurring common costs during that year, which shall be allocated on the basis of the allocation key referred to in paragraph (97)(c). ([18])

(95) Only incremental costs that are clearly attributable to making the Search Data available shall qualify for the purpose of determining the compensation. Costs shall not qualify merely because they arise in connection with the obligation. Alphabet shall be able to demonstrate that all incremental cost items are objective, measurable, verifiable and proportionate to the purpose of making the data available. Overhead, sunk costs, investments in data collection, processing and storage not attributable to making the Search Data available, speculative risks, ordinary business and general compliance expenses, or dispute-related legal costs do not qualify for inclusion in the

([17]) No return on capital shall be due after a beneficiary has paid the fixed fee.

([18]) For the purposes of calculating the fee Alphabet may charge for accessing the data samples B and C, as referenced in sections 5.1.2 and 5.1.3, Alphabet should only take into account recurring beneficiary-specific costs.

cost base to identify the incremental cost incurred by Alphabet in the process of making the Search Data available to eligible beneficiaries.

(96) Incremental costs related to the development, set-up and scaling of the data sharing mechanism, shall be considered as capital employed for the purpose of making the Search Data available to the extent that they reflect expenditures for the development of assets, systems or capabilities that are expected to be used over multiple years.

(97) One-off and recurrent incremental cost items that are common to different beneficiaries shall be allocated in a reasonable, transparent and predictable manner, having regard to the nature of the relevant cost item and the point in time at which it is incurred. The volume of access requests cannot be known in advance and may vary over time. The allocation methodology shall not result in unjustified differences in treatment between beneficiaries obtaining access at different points in time. To this effect, Alphabet shall:

(a) determine the initial per-beneficiary share of the one-off costs based on a reasonable and justified estimate of the expected number of beneficiaries at the time the access mechanism is first made available, as determined following the process described in section 5.4.2, with those costs to be shared equally among all such expected beneficiaries;

(b) apply the same fixed component, as described under paragraph (94) and established following the methodology laid out in point (a), to all actual beneficiaries irrespective of the time they start having access, subject only to differences objectively justified by beneficiary-specific one-off costs; ([19])

(c) recurrent common costs shall be shared equally among the beneficiaries receiving access during a given year.

(98) In line with section 5.4.2, upon request, Alphabet shall provide information setting out the basis for the calculation of the compensation in sufficient detail so that eligible beneficiaries can assess whether the above-stated requirements are met. Alphabet shall maintain, for each year, information supporting the calculation of the compensation and, upon request of the beneficiaries, provide them with a non-confidential version thereof, at the appropriate level of granularity, to ensure both a sufficient degree of transparency as well as the protection of confidential information. Confidential and non-confidential versions of the information setting out the basis for the calculation of the compensation shall also be provided to the Commission.

(99) Alphabet shall attempt to resolve any disagreement on the application of the above-specified calculation methodology directly with beneficiaries in good faith. Should a disagreement on any elements of the compensation persist, Alphabet shall not prevent beneficiaries from raising such disagreement with the Commission. The Commission reserves the right to take action in accordance with its powers under Regulation (EU) 2022/1925 to verify Alphabet's compliance with the above terms, including auditing Alphabet's costs to ensure that they are reasonable and proportionate to the claimed expenses. This provision is without prejudice to the beneficiaries' right to initiate legal proceedings before the competent courts.

([19]) For instance, where additional eligible beneficiaries obtain access after the initial intake period, those beneficiaries shall be subject to the same fixed component corresponding to one-off common costs as beneficiaries that obtained access earlier, subject only to adjustments reflecting objectively justified beneficiary-specific one-off costs.

(100) Regarding eligible beneficiaries that are also designated gatekeepers under Article 3(4) Regulation (EU) 2022/1925 in relation to an online search engine core platform service, Alphabet may deviate from the FRAND compensation specified in this Decision. In that case, Alphabet shall still negotiate, in good faith, and within the limits set out in Article 6(11) of Regulation (EU) 2022/1925, the applicable compensation provided that any resulting terms, considering the relevant circumstances and position of the two parties, remain FRAND within the meaning of Article 6(11) of Regulation (EU) 2022/1925 and otherwise comply with that provision.

5. PROCESS FOR SEARCH DATASET ACQUISITION AND PRE-ACQUISITION DATA TESTING

5.1. Process and practical arrangements for pre-acquisition technical testing

(101) Alphabet shall give third-party OSEs the opportunity to conduct technical testing on test data samples before they agree to acquire the Search Dataset.

(102) Alphabet shall provide three different test data samples to any eligible third-party OSE applying for eligibility to test data samples or the Search Dataset. Each test data sample shall have a different scope in terms of content as well as means and conditions of access. These are:

(a) **Sample A:** Alphabet shall continue to provide a small sample of 1 000 rows (i.e., 58 unique queries) from the Search Dataset;

(b) **Sample B:** Alphabet shall provide a synthetic dataset that eligible third-party OSEs may download onto their own servers to conduct technical testing; and

(c) **Sample C:** Alphabet shall provide a large representative sample dataset that eligible third-party OSEs may download onto their own servers to conduct technical testing.

5.1.1. Sample A – access arrangements, access conditions and content

(103) Alphabet shall continue to provide a 1 000-row sample (i.e., 58 unique queries) of the Search Dataset free of charge ("**Sample A**"). Alphabet shall continue to allow third-party OSEs to download Sample A onto their own servers free of charge.

(104) Alphabet may impose a contractual restriction preventing the third-party OSE from sharing Sample A with any other person or undertaking. Alphabet shall otherwise make Sample A available under the same conditions it makes the small Alphabet sample available.

5.1.2. Sample B – access arrangements, access conditions and content

(105) Alphabet shall prepare a synthetic dataset of 10 million individual representative artificially generated unique queries (also often called "synthetic" queries) and metadata ("**Sample B**") and provide this to any third-party OSE that requests it. Alphabet shall comply with any request from a third-party OSE that the copy of Sample B it receives contain a particular number of queries and associated metadata, up to a maximum of 10 million individual queries.

(106) Alphabet shall allow third-party OSEs to download Sample B onto their own servers. Alphabet may impose a contractual restriction preventing the third-party OSE from sharing Sample B with any other person or undertaking.

(107) Alphabet shall not make access to Sample B conditional on the third-party OSE in question providing any assurance report specified in section 3.2.4 or undergoing an audit associated with this assurance report. Alphabet may only grant Sample B to a third-party OSE that it has deemed a third-party OSE eligible to receive the Search Dataset in accordance with section 1.

(108) Alphabet shall explain, in a clear and transparent manner, the method by which it produced Sample B. Alphabet shall ensure that Sample B is a faithful representation of the real Search Dataset to which technical measures specified in section (26) have been applied. This means, among other things, that Sample B shall:

(a) Accurately resemble the real Search Dataset in content and form;

(b) Faithfully reflect the relationship between queries and metadata;

(c) Include all the data fields specified in section 2; and

(d) Have the technical measures specified in section 3.1 applied in the same way they would be applied to the real Search Dataset.

(109) Alphabet may limit the time during which third-party OSEs may retain Sample B. This retention period shall be a period of at least three months from the date on which Sample B was first made available to that third-party OSE.

(110) Alphabet may charge third-party OSEs a fee for accessing Sample B. This fee shall be calculated using the method specified in section 4.

5.1.3. Sample C – access arrangements, access conditions and content

(111) Alphabet shall provide a sample of 5% of the final Search Dataset selected from queries occurring in no less than one month and no more than one year ("**Sample C**") (with the exact period to be specified by the third-party OSE requesting Sample C).

(112) Alphabet shall provide Sample C once the Search Dataset is finalised in accordance with section 5.2 and all applicable conditions for the sharing of the Search Dataset have been met by the third-party OSE. Alphabet shall require third-party OSEs to apply the retention period specified in section 3.2.2 to Sample C.

(113) Alphabet may charge third-party OSEs a fee for accessing Sample C. This fee shall be calculated using the method specified in section 4.

(114) Alphabet shall comply with any requests from any third-party OSE that all queries in the Sample C dataset it accesses:

(a) Come from a particular Member State or Member States of the EU;

(b) Be in a particular language or languages; or

(c) Take place within a particular period of no less than one month.

5.2. Process for finalising the Search Dataset

(115) Alphabet shall finalise the Search Dataset as soon as possible and no later than four months after the Commission's adoption of these measures. Alphabet shall notify the Commission as soon as it has finalised the Search Dataset. This notification shall describe the actions Alphabet has taken to implement the measures specified in sections 2.1, 2.2 and 3.1.

(116) Within four months of the adoption of these measures, Alphabet shall share a document with the Commission setting out:

(a) The final latency of Search Data sharing along with the technical description and justification, as specified in section 2.2.2; and

(b) The information on personal data detectors and list of result types specified at section 3.1, paragraph (41).

5.3. Process for finalising the licence agreements for the Search Dataset and the test data samples

(117) Alphabet shall prepare a template licence agreement for the sharing of the Search Dataset with third-party OSEs, implementing all applicable provisions of the measures specified, within two months of the Commission's adoption of these measures.

(118) Alphabet shall also prepare template licence agreements for sharing Sample A, Sample B and Sample C within two months of the Commission's adoption of these measures.

(119) Within one working day of finalising the template licence agreements, Alphabet shall share a copy of each template licence agreement with any undertaking applying for eligibility, eligible third-party OSE and the Commission.

(120) The Search Dataset and Sample C template licence agreements shall allow a third-party OSE to specify that all queries forming part of the Search Dataset or Sample C dataset it receives come from a particular Union Member State or Member States, be in a particular language or take place within a period of no less than one month.

(121) Alphabet may only impose conditions for sharing the Search Dataset or test data samples that are FRAND and strictly proportionate. These conditions shall not impede in any way the effectiveness of these Measures or the Commission's Decision in this case.

5.4. Processes for making the Search Dataset available, reviewing eligibility of undertakings applying for eligibility, finalising pricing terms and ensuring continuity of access

5.4.1. Process for providing Search Dataset(s) and reviewing eligibility of undertakings applying for eligibility

(122) Alphabet shall engage with any undertaking applying for eligibility to determine whether it is eligible to receive the Search Dataset.

(123) Alphabet shall put in place a structured, adequately documented process setting out how it will receive, acknowledge, assess and respond to applications for eligibility and requests for the Search Dataset and test data samples.

(124) To this end, within 45 days of the adoption of these measures, Alphabet shall provide a publicly accessible webpage containing up-to-date information including:

(a) A clear explanation of Alphabet's obligations under Article 6(11) of Regulation (EU) 2022/1925 specified in these Measures; and

(b) Clear and detailed information on how to contact Alphabet with a view to submitting a request for the Search Dataset.

(125) Alphabet shall reply to any expressions of interest in acquiring the Search Dataset within one week. This reply shall contain at least the following information:

(a) An application form with clear and detailed information the undertaking applying for eligibility is to provide in order to enable Alphabet to make the eligibility assessment under section 1, paragraphs (3) - (7);

(b) A description of the Search Dataset, test data samples and the process and basis under which FRAND prices will be calculated in accordance with sections 4 and 5.4.2;

(c) Clear and detailed information regarding:

(1) Process for assessing eligibility;

(2) The requirement to submit the Level 1 reasonable assurance report as a condition for being granted initial access to the Search Dataset, and the requirement to submit the Level 2 reasonable assurance report as a condition for maintaining access to the Search Dataset in accordance with the conditions specified in section 5.4.3; and

(3) Processes for granting access to, ensuring continuity of access to, refusing access to, suspending access to and terminating access to the Search Dataset;

(d) Copies of the template licence agreements in respect of the Search Dataset, Sample A, Sample B and Sample C; and

(e) An e-mail address (to be communicated by the Commission to Alphabet) at which the undertaking applying for eligibility may contact the Commission to provide information or submit questions regarding Alphabet's sharing of the Search Dataset.

(126) Alphabet shall present a draft of this application form (including eligibility questionnaire) to the Commission within 45 days of the Commission's adoption of these measures.

(127) Alphabet shall require the submission of a Level 1 assurance report consisting solely of a **non-confidential version containing the assurance conclusions** of the qualified independent assurance practitioner and confirming that reasonable assurance has been obtained for each of the three assurance objectives defined in section 3.2.4.3.

(128) Alphabet shall require all eligible third-party OSEs to notify Alphabet as soon as they have entered into a contract with an auditor for the purposes of preparing a Level 1 assurance report.

(129) Alphabet shall limit its verification of the Level 1 assurance report to confirming the submission of the report and its formal completeness, meaning that the report is issued by a qualified independent assurance practitioner and contains the assurance conclusions for each of the three assurance objectives defined in section 3.2.4.3 in the prescribed non-confidential format. Alphabet shall not reassess the substance or scope of the assurance conclusions expressed by the qualified independent assurance practitioner. Within two weeks of receiving the Level 1 reasonable assurance report (in the case of the Search Dataset and Sample C) and signed licence agreement (in respect of the Search Dataset and all test data samples), Alphabet shall either:

(a) Provide the Search Dataset or test data sample in question to the undertaking applying for eligibility; or

(b) Send the undertaking applying for eligibility a decision rejecting the report in accordance with section 5.5.1.

(130) Alphabet shall inform the Commission of any request it receives without delay. Alphabet shall conclude its eligibility assessment within one week of receipt of a completed application form (including eligibility questionnaire) and transfer impact assessment, if applicable).

(131) Alphabet shall grant access to the Search Dataset to each eligible third-party OSE within 10 days after it has entered into a licence agreement and accepted the price offer, which is to be finalised within six months of the adoption of these measures in accordance with section 5.4.2.

5.4.2. Process for finalising pricing terms

(132) The Commission specifies the following process for finalising Alphabet's pricing terms and communicating them to third-party OSEs applying for eligibility and, ultimately, to eligible beneficiaries.

(133) Without prejudice to the obligation outlined in paragraph (98), within two months of the adoption of these measures, Alphabet shall submit the following elements:

(a) An exhaustive list of cost items and estimates, as well as a description of the nature of the respective items (e.g., WACC , one-off or recurring cost, fixed or variable cost, beneficiary-specific or common, whether the cost items scale with the volume or frequency of data to be shared and to what cost category among the ones listed in (91) it relates to).

(b) A detailed description of the methodology underlying the pricing calculations it has prepared in accordance with section 4, including, but not restricted to:

(1) A description of the methodology used to calculate the WACC, which the reasonable return on the capital employed for the purpose of making the Search Data available cannot exceed.

(2) A description of the methodology used to calculate the margin as used in the pricing scenario laid out in paragraph (88).

(3) Any element that remains contingent on the number of eligible beneficiaries, including the allocation of one-off common costs, the applicable formulas, calculation steps and assumptions. ([20])

(134) In line with paragraph (98), Alphabet shall provide confidential and non-confidential versions of the information outlined in paragraph (133) to the Commission. Alphabet shall share non-confidential versions of such information, at the appropriate level of granularity to ensure both a sufficient degree of transparency as well as the protection of confidential information, with third-party OSEs applying for eligibility. ([21])

(135) Within six months of the adoption of these measures, Alphabet shall provide the Commission with, and communicate to all third-party OSEs that have either (i) applied for eligibility and entered into a contract with an auditor for the purposes of

([20]) Alphabet shall indicate how the number of eligible beneficiaries, and any subsequent change thereof, will affect the final amount charged to each eligible beneficiary once known.

([21]) "Third-party OSEs applying for eligibility" shall have the same meaning as "undertakings applying for eligibility" as defined in paragraph (3)(a).

preparing a Level 1 assurance report, or (ii) have been assessed as eligible to receive the Search Data following the criteria laid out in section 1:

(a) The number of third-party OSEs that have either applied for eligibility and informed Alphabet that they have entered into a contract with an auditor for the purposes of preparing a Level 1 assurance report, or have been assessed as eligible to receive the Search Data; and

(b) The resulting pricing offers, including an allocation of one-off common costs divided equally among third-party OSEs applying for eligibility that have entered into such a contract with an auditor or that have been assessed as eligible to receive the Search Data, following the allocation key laid out in paragraph (133)(b)(3).

(136) The Commission may prolong the six-month period where the proposed methodology in paragraph (87) is not deemed appropriate, or where technical or procedural issues have delayed the effective preparation, assessment or implementation of the pricing offer.

(137) The communication of the pricing offers pursuant to paragraph (135) shall be without prejudice to the Commission's assessment of whether Alphabet's methodology complies with these measures and with Article 6(11) of Regulation (EU) 2022/1925.

(138) If the Commission is of the opinion that Alphabet's calculations are not compliant with these measures or with Article 6(11) of Regulation (EU) 2022/1925, Alphabet shall comply with any directions from the Commission to submit new calculations or other information necessary to calculate FRAND pricing offers within any time limit stipulated by the Commission.

5.4.3. Submission of Level 2 assurance reports to maintain access to the Search Dataset

(139) As a condition for maintaining access to the Search Dataset, Alphabet shall require the third-party OSE to submit to Alphabet, on an annual basis, the Level 2 assurance report in accordance with the conditions specified in section 3.2.4:

(a) For the first Level 2 assurance report, within six months of the date the third-party OSE first received access to the Search Dataset;

(b) For all subsequent Level 2 assurance reports, within 12 months of the date on which the previous Level 2 assurance report was submitted.

(140) In addition, Alphabet shall require the third-party OSE to submit to Alphabet, on an *ad hoc* basis, a Level 2 report where it receives a written notification from the Commission confirming that the Commission is of the opinion that such a report is required in the circumstances. Alphabet shall not require any third-party OSE to submit an *ad hoc* Level 2 report unless it has received such written notification from the Commission. Alphabet shall also require the third-party OSE to submit this *ad hoc* Level 2 report by a time limit stipulated by the Commission in the Commission's written notification to Alphabet. The decision on whether an *ad hoc* Level 2 report is required, and the time limit for submitting this report, shall be solely for the Commission in each instance. If a third-party OSE submits an *ad hoc* Level 2 report concluding reasonable assurance, Alphabet shall not require the third-party OSE to submit any further Level 2 report in the period of less than 12 months from the date of submission of the *ad hoc* Level 2 report.

(141) The Level 2 assurance report shall consist solely of a **non-confidential version containing the assurance conclusions** of the qualified independent assurance practitioner confirming that reasonable assurance has been obtained in relation to each of the three assurance objectives defined in section 3.2.4.3.

(142) Alphabet shall limit its verification to confirming the submission of the report and its formal completeness, meaning that the report is issued by a qualified independent assurance practitioner and contains the assurance conclusions for each of the three assurance objectives defined in section 3.2.4.3 in the prescribed non-confidential format. Alphabet shall not reassess the substance or scope of the assurance conclusions expressed by the qualified independent assurance practitioner.

(143) Failure to submit a Level 2 assurance report within the applicable time limits, or failure of the submitted report to confirm that reasonable assurance has been obtained (where the independent assurance practitioner issues a "limited assurance" conclusion), shall lead to a suspension decision and/or a termination or expedited decision in accordance with sections 5.5.2.1 and 5.5.3. For the avoidance of doubt, this provision shall also extend to the submission of *ad hoc* Level 2 reports.

5.4.4. Prior notification of a change of control and submission of Level 1 reasonable assurance reports to ensure continuity of access following a change of control of the third-party OSE

(144) Alphabet shall require written notification from the third-party OSE of any intended change of control over the third-party OSE (including acquisitions of joint control or sole control or changes in the quality of control) within 10 days after it becomes public or at least 30 days prior to the change taking effect, whichever is earlier. Alphabet shall transmit the notification to the Commission upon receipt.

(145) Alphabet shall require the notification to identify the natural or legal person(s) acquiring control of the third-party OSE. If this information is not publicly available and is commercially sensitive, Alphabet shall require the third-party OSE to notify the Commission directly and share a non-confidential version of the notification with Alphabet.

(146) Alphabet may conduct a new eligibility assessment in accordance with sections 1 and 5.4.1 if it believes based on credible, objective evidence that the change in control could impact on the third-party OSE's eligibility to receive the Search Dataset. Alphabet shall conclude this eligibility assessment within one week of receipt of a completed due diligence questionnaire and transfer impact assessment, if applicable.

(147) Subject to this eligibility assessment, following a change of control of the third-party OSE, Alphabet shall ensure that the third-party OSE continues to receive access to the Search Dataset immediately after the third-party OSE and the person or persons acquiring control (together the "**merging parties**") submit a new Level 1 reasonable assurance report that takes the change of control into account. Alphabet may only terminate access to the Search Dataset following a change of control of a third-party OSE in accordance with the conditions set out in sections 5.5.2, 5.5.3 and 5.5.4.

5.4.5. Submission of Level 2 reasonable assurance reports to ensure continuity of access following the commencement of insolvency proceedings

(148) Alphabet shall require written notification from the third-party OSE of any insolvency proceedings initiated against it within one week of the initiation of those proceedings. Alphabet shall transmit the notification to the Commission upon receipt.

(149) The notification shall identify the jurisdiction and court in which proceedings were brought and briefly describe the circumstances precipitating the proceedings. If this information is not publicly available and is commercially sensitive, Alphabet shall require the third-party OSE to notify the Commission directly and share a non-confidential version of the notification with Alphabet.

(150) Following the initiation of insolvency proceedings, Alphabet shall ensure that the third-party OSE continues to receive access to the Search Dataset immediately after the third-party OSE submits a Level 2 reasonable assurance report that takes the insolvency proceedings into account.

(151) Alphabet may only suspend access to the Search Dataset following initiation of insolvency proceedings in accordance with the conditions set out in section 5.5.2.1.

5.5. Processes for refusing, suspending and terminating access to the Search Dataset

5.5.1. Refusal decisions

(152) If Alphabet decides either:

(a) To deny an undertaking applying for eligibility from accessing the Search Dataset; or

(b) To deny an undertaking applying for eligibility from accessing a test data sample,

it shall send the undertaking applying for eligibility a written notification refusing access to the Search Dataset (the "**refusal decision**") by the applicable deadline set out in section 5.4.1.

(153) The refusal decision shall include at least the following:

(a) **Reasoning:** an explanation of the grounds for the refusal decision;

(b) **Rebutting evidence:** an explanation of the evidence the undertaking applying for eligibility shall provide to rebut the refusal decision; and

(c) **Contact:** who the undertaking applying for eligibility can contact and how if it has any questions on the refusal decision.

5.5.2. Suspension of access

5.5.2.1. Measures for suspension

(154) Alphabet shall suspend an individual third-party OSE's access to the Search Dataset in the following circumstances:

(a) **Failure to submit a Level 2 reasonable assurance report on time:** the third-party OSE does not submit a Level 2 reasonable assurance report within the time limit specified in section 5.4.3 (or as specified by the Commission in the case of *ad hoc* audits), or submits a Level 2 report concluding limited assurance; or

(b) **Insolvency:** insolvency proceedings in respect of the third-party OSE are opened.

(155) Alphabet shall notify the third-party OSE in writing no more than three days after the suspension ("**suspension decision**"). The suspension decision shall contain at least the following:

(a) **Reasoning:** a clear and detailed explanation of the grounds for the suspension;

(b) **Effects:** a description of the legal and operational consequences of the suspension;

(c) **Remediation:** a clear and detailed explanation of the evidence the third-party OSE shall provide to restore its access to the Search Dataset; and

(d) **Alphabet's obligation to terminate:** the conditions under which Alphabet shall terminate access to the Search Dataset specified in section 5.5.3.

5.5.2.2. Measures for restoration of access to the Search Dataset

(156) Alphabet shall reverse a suspension and restore the third-party OSE's access to the Search Dataset as soon as technically possible once the third-party OSE has remedied the circumstances that triggered the suspension or has otherwise demonstrated that those circumstances no longer apply, in accordance with the conditions set out below.

(157) In particular, Alphabet shall restore access to the Search Dataset in the following circumstances:

(a) **Failure to submit a Level 2 reasonable assurance report on time:** where the third-party OSE submits to Alphabet a Level 2 reasonable assurance report in accordance with section 5.4.1;

(b) **Submission of a Level 2 assurance report concluding limited assurance:** where the third-party OSE submits to Alphabet a supplemental reasonable assurance report confirming that reasonable assurance has now been obtained for the assurance objectives previously assessed as limited; and

(c) **Insolvency:** where the third-party OSE provides an updated Level 2 reasonable assurance report which takes any relevant changes to the third-party OSE's business that relate to the insolvency proceedings into account.

5.5.3. Termination following suspension

(158) Alphabet shall decide to permanently terminate an individual third-party OSE's access to the Search Dataset ("**termination measure**") in the below specified circumstances where a third-party OSE fails to provide the evidence of remediation specified in section 5.5.2.2 within three months of receiving the suspension decision specified in section 5.5.2.1.

(159) Within five working days after it has terminated access, Alphabet shall send the third-party OSE a decision which includes at least the following:

(a) **Reasoning:** a detailed explanation of the grounds for the termination decision; and

(b) **Effects:** a detailed explanation of the legal consequences of the termination decision.

(160) Upon issuing a termination decision, and unless a supervisory authority has opened an investigation or taken investigative steps under Regulation (EU) 2016/679 against the third-party OSE that require the retention of the Search Dataset as evidence, Alphabet shall take all necessary contractual measures to ensure:

(a) That the party subject to the termination decision:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset;

and

(b) That any other third party to whom the party subject to the termination decision disclosed (whether intentionally or not) the Search Dataset:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset.

(161) Alphabet shall take all necessary steps to ensure these contractual measures are enforced (including appropriate audit measures to verify erasure, at Alphabet's own expense).

(162) Alphabet shall allow third-party OSEs that have been subject to a termination or expedited termination measure to re-apply for access to the Search Dataset. Alphabet shall treat any such subsequent application for the Search Dataset as if it were an application from a new undertaking applying for eligibility. Where a terminated third-party OSE successfully reapplies for the Search Dataset, Alphabet shall take into account any past payments of that third-party OSE towards the fixed fee specified in section 4.

5.5.4. Expedited termination

(163) Alphabet may decide to issue termination decisions in exceptional circumstances without following the procedures and time limits specified in sections 5.5.2 and 5.5.3 ("**expedited termination decisions**").

(164) Alphabet may only issue an expedited termination decision in the following three circumstances:

(a) **Integrity and confidentiality of the Search Dataset:** where Alphabet becomes aware of substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised;

(b) **Failure to submit a Level 1 reasonable assurance report in the case of a change of control:** the merging parties fail to submit a Level 1 reasonable assurance report before the change of control takes effect;

(c) **Failure to notify a change of control:** the merging parties fail to notify a change of control within 10 days after it becomes public or at least 30 days prior to the change taking effect (whichever is earlier) in accordance with section 5.4.4.

(165) The expedited termination decision shall include at least the following:

(a) **Reasoning:** a detailed explanation of the grounds for the expedited termination decision including all substantiated evidence demonstrating that the integrity and confidentiality of the Search Dataset has been compromised; and

(b) **Effects:** a detailed explanation of the legal consequences of the termination decision or expedited termination decision.

(166) To enable supervisory authorities to exercise their functions under Regulation (EU) 2016/679 in the event of expedited termination, Alphabet shall take all necessary contractual measures to ensure that the third-party OSE retains the Search Dataset for a period of four weeks following the third-party OSE's receipt of a termination decision.

(167) Upon the expiry of this four-week period, and unless a supervisory authority has opened an investigation or taken investigative steps under Regulation (EU) 2016/679

against the third-party OSE that require the retention of the Search Dataset as evidence, Alphabet shall take all necessary contractual measures to ensure:

(a) That the party subject to the termination decision:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset;

and

(b) That any other third party to whom the party subject to the termination decision disclosed (whether intentionally or not) the Search Dataset:

(1) Erases all of the Search Dataset under its control; and

(2) Does not further process or share the Search Dataset.

(168) Alphabet shall take all necessary steps to ensure these contractual measures are enforced (including appropriate audit measures to verify erasure, at Alphabet's own expense).

5.6. Requirement to impose financial penalties in exceptional circumstances

(169) Alphabet shall impose strictly necessary and proportionate financial penalties on a third-party OSE in the following instances:

(a) A third-party OSE fails to notify a change of control in accordance with section 5.4.4;

(b) A third-party OSE fails to notify the commencement of insolvency proceedings against it in accordance with section 5.4.5;

(c) A third-party OSE fails to notify Alphabet that it has received a limited assurance report;

(d) A third-party OSE fails to comply with the necessary contractual measures imposing erasure of the Search Dataset as per section 5.5.3 and 5.5.4; or

(e) A third-party OSE provides materially false information to Alphabet in connection with the independent verification mechanism specified at section 3.2.4.

(170) Alphabet shall not impose financial penalties on third-party OSEs in relation to their processing of the Search Dataset.

5.7. Requirement to amend documents and obligation to inform the Commission, data protection supervisory authorities and the public of decisions granting, refusing, suspending, restoring or terminating access

(171) The Commission may require Alphabet to amend the documents that it shall produce to implement the present specification within a deadline to be set by the Commission if the Commission finds that these documents do not effectively comply with Article 6(11) of Regulation (EU) 2022/1925 and the measures in the present specification. This includes the documents referred to in paragraphs (117), (125)(a), (133) and (135).

(172) Alphabet shall share a copy of any refusal, suspension or termination decision with the Commission at the same time it shares any such refusal, suspension or termination decision with the third-party OSE in question.

(173) Alphabet shall also share a copy of any suspension or termination decision with the lead supervisory authority at the same time it shares any such suspension or termination decision with the third-party OSE in question. Throughout these Measures, *"lead supervisory authority"* means the lead supervisory authority for the processing carried out by the third-party OSE in line with Article 56(1) of Regulation (EU) 2016/679.

(174) Alphabet shall inform the Commission and the lead supervisory authority within five working days of any restoration of access to the Search Dataset following a suspension. It shall also provide the reasons for which it has restored access to the Search Dataset.

(175) Alphabet shall notify the Commission and the lead supervisory authority of the third-party OSE of its intention to issue an expedited termination decision at least three working days before it intends to issue such expedited termination decision to the third-party OSE in question. In its notification, Alphabet shall clearly explain the reasons for its expedited termination decision and provide supporting evidence.

(176) Alphabet shall maintain on its website a page listing all third-party OSEs that have received access to the Search Dataset. Alphabet shall display on this page a notice in respect of each eligible third-party OSE publicising that Level 1 and Level 2 assurance has been obtained as well as a notice publicising the fact of any termination and expedited termination decisions, as well as a short description of the reasons for such termination or expedited termination decisions. These notices shall not contain any information which is confidential information or business secrets of the third-party OSE.

***