Reconciling Competition and Privacy in Accessing Search Data in Europe

Dr Christophe Carugati

In Europe, Google Search must grant rivals access to search data. In its specification proceeding, the Commission can define the scope of data, the anonymisation method, and access conditions to reconcile competition and privacy.

Introduction

European policymakers seek to ensure effective competition in general search engines while safeguarding user privacy. General search engines, such as Google Search and Microsoft Bing, collect both personal and non-personal data, including search queries, to provide relevant results for users. According to policymakers, access to such data provides large search engine providers with a competitive scale advantage, which may constitute a barrier to entry and expansion for rival providers that cannot match their search quality due to insufficient search data.

The Digital Markets Act (Regulation (EU) 2022/1925, DMA) seeks to ensure contestability by imposing obligations on designated large online platforms considered as "*gatekeepers*." As of March 2026, only Google Search has been designated as a gatekeeper for the provision of general search services[1]. Among the relevant obligations, the search data access requirement of Article 6(11) aims to reduce this scale advantage by requiring Google Search to grant competing providers access to search data generated by end users, including ranking, query, click, and view data, under fair, reasonable, and non-discriminatory (FRAND) terms, provided that personal data is anonymised to protect user privacy.

However, these privacy and competition objectives may conflict. As recognised by the legislator in Recital 61, anonymisation safeguards privacy but may degrade the quality or usefulness of the data that competing providers need to improve their services. In 2024, DuckDuckGo, a rival, claimed that Google's proposed data-sharing framework eliminated 99%

[1] For the list of designated gatekeepers, *See* Gatekeepers, *European Commission* (accessed 10 March 2026). Available at: https://digital-markets-act.ec.europa.eu/gatekeepers_en

of search queries through anonymisation, rendering the dataset less useful for improving competing search services[2]. Over the past three years, Google has stated in its annual compliance reports that it complies with the obligation and has progressively expanded the data available to data recipients through new technical approaches[3].

In January 2026, the European Commission opened two specification proceedings against Google relating to the search data access and interoperability obligations. The search data access proceeding focuses on the scope of data to be shared, the anonymisation method, the conditions of access, and whether providers of Artificial Intelligence (AI) chatbots should be eligible to receive the data[4].

Against this background, this analysis provides a high-level overview of the search data access obligation, reconciling privacy and competition when granting access to search data. It first examines the interaction between competition and privacy, then analyses the coherent application of both objectives, and finally proposes policy recommendations for the Commission's ongoing proceeding.

Interaction Between Competition and Privacy

The search data access obligation simultaneously promotes competition and protects privacy. From a competition perspective, access to search data can reduce the scale advantage enjoyed by large search engines, enabling rival providers to improve the quality of their services. From a privacy perspective, anonymisation protects end users against the risk of re-identification.

However, these objectives create inherent tensions. Promoting competition depends on both the scope of data made available to recipients and the conditions of access. Maximising competition would require granting access to a broad set of search queries, encompassing different types of data (personal and non-personal), contexts (such as the search results surrounding each query), and characteristics (including freshness, utility, scale, and variety).

[2] Roadblocks to Competition: Investigate Google's Non-Compliance with the EU's Digital Markets Act, *DuckDuckGo*, 20 November 2024 (accessed 10 April 2026). Available at: https://spreadprivacy.com/investigate-google-dma/

[3] Compliance Report under the European Union Digital Markets Act (EU DMA), *Alphabet* (accessed 10 March 2026). Available at: https://transparencyreport.google.com/?hl=en

[4] Commission Opens Proceedings to Assist Google in Complying with Interoperability and Online Search Data Sharing Obligations Under the Digital Markets Act, *European Commission*, 27 January 2026 (accessed 10 March 2026). Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_202

Providing access to personal data must comply with the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR). The regulation sets strict data processing requirements of lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and accountability (Article 5). In particular, the lawfulness principle implies informing users transparently and a legal basis for processing, such as consent, contractual necessity, legal obligation, vital interest, public interest, or legitimate interest (Article 6).

The DMA requires gatekeepers to provide access to both free and paid search data on FRAND terms, but does not specify the precise scope of the data or the conditions of access. With respect to personal data, the regulation neither establishes a lawful basis for processing nor requires that users be informed of the sharing of their data with third-party recipients. For this reason, the DMA mandates that personal data be anonymised prior to sharing, so that the GDPR no longer applies, as anonymised data fall outside its scope (Recital 26). However, anonymisation necessarily reduces the scope of available data.

Achieving privacy protection, therefore, depends on the anonymisation method employed. Recital 61 of the DMA specifies that effective anonymisation requires personal-related queries to be irreversibly altered to prevent identification. Re-identification risks include single-out (isolating an individual), linkability (connecting records to reveal identity), and inference (deducing personal attributes)[5]. Addressing these risks inevitably reduces data quality. In practice, it leads to the removal of certain queries, particularly rare or unique queries (so-called "*tail queries*"), which are important for generating relevant search results, as recognised in the Commission's *Google Search (Shopping)* decision[6]. In particular, removing such queries reduces the risk that recipients could link the dataset with their own data to re-identify users, a risk heightened by the low frequency of personal-related queries. Recital 61 further provides that anonymisation should not substantially degrade the quality or usefulness of the data.

The DMA thus requires gatekeepers to implement anonymisation methods that effectively mitigate re-identification risks, without specifying the techniques to be used. From a legal perspective, ensuring effective anonymisation must take precedence over preserving data quality. The extent to which data quality can be maintained depends on the state of the art in anonymisation methods, including technical and non-technical measures. For example, in its

[5] For a deeper discussion on anonymisation techniques, *See* Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, 10 April 2014 (accessed 10 March 2026). Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[6] Case AT.39740 *Google Search (Shopping)*, 27 June 2017, para. 288.

March 2026 compliance report, Google indicates that it applies frequency-thresholding techniques to remove rare queries that could otherwise enable re-identification[7].

In this context, reconciling privacy and competition largely depends on the anonymisation method adopted, applied coherently to meet both objectives.

Coherence Between Competition and Privacy

Ensuring coherence between competition and privacy rules is essential to provide legal certainty for both gatekeepers and data recipients. In October 2025, the Commission and the European Data Protection Board (EDPB) issued draft joint guidelines on the interaction between the DMA and the GDPR. Among other objectives, the guidelines clarify how anonymisation can support contestability while protecting user privacy[8].

The draft guidelines emphasise the choice of anonymisation method. Gatekeepers should select techniques that preserve the highest possible quality and usefulness of the data while considering all means reasonably likely to be used to identify end users, directly or indirectly. Effective anonymisation should combine technical measures that modify the dataset with organisational, administrative, and contractual safeguards that reduce residual identification risks[9].

However, the draft guidelines do not detail an anonymisation method. Instead, they note that the Commission may adopt an implementing act following a specification proceeding under Article 8(2) of the DMA to determine the appropriate technical and non-technical measures, while only providing high-level guidance on their design[10].

The guidelines also indicate that FRAND access conditions should not impose disproportionate burdens on recipients, including in terms of costs. Nevertheless, they provide little detail

[7] EU Digital Markets Act (EU DMA) Compliance Report Non-Confidential Summary, *Google*, 6 March 2026, p. 199.

[8] European Commission and EDPB, Joint Guidelines on the Interplay Between the Digital Markets Act and the General Data Protection Regulation, 9 October 2025 (accessed 10 March 2026). Available at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_en

[9] *Ibid*, paras 180 and 181.

[10] *Ibid*, paras. 188-189.

regarding the types of obligations that gatekeepers may impose on data recipients to mitigate re-identification risks[11].

These issues are therefore likely to be central to the Commission's ongoing specification proceeding.

Policy Recommendations

The specification proceeding offers an opportunity to provide greater legal certainty regarding the anonymisation framework. The Commission will soon issue its preliminary findings on the measures it may impose to ensure Google's effective compliance with Article 6(11). In this context, the Commission should follow three recommendations to reconcile competition and privacy for access to search data.

First, it should maximise the usefulness of the data to promote competition. When defining the scope of accessible data, the Commission should identify both personal and non-personal data that are relevant to recipients, taking into account the "four Vs" of data, namely volume, variety, velocity, and value, as well as the contextual relevance of queries[12]. This would ensure that rival providers can effectively improve the quality of their search services.

Second, it should ensure effective anonymisation to protect privacy. The specification of the anonymisation method should account for state-of-the-art technical safeguards that reduce re-identification risks while preserving data quality. The approach should also consider the context in which the data will be accessed and used to avoid re-identification risks.

Third, it should impose targeted obligations on data recipients to mitigate residual privacy risks. The access conditions should require data recipients to implement internal controls to restrict data use, report potential incidents, and undergo independent audits. At the same time, the Commission should avoid imposing disproportionate monitoring obligations on gatekeepers once access has been granted, as they cannot effectively oversee how recipients process the data.

[11] *Ibid*, para. 190.

[12] The Commission has already deeply assessed these "4 Vs" of data in the *Apple/Shazam* merger. *See*, M.8788 *Apple/Shazam*, 6 September 2018.

About

Digital Competition

Digital Competition (https://www.digital-competition.com/) is a digital and competition expert services for businesses, law firms, and government agencies, dedicated to promoting open digital and competition policies that foster innovation. Led by Dr. Christophe Carugati, a passionate and impartial expert in digital and competition policy, we bring together legal, economic, and policy expertise to deliver cutting-edge research, strategic advice, think tank initiatives, regulatory intelligence, tailored training, and high-impact conferences. Digital Competition is committed to addressing the most pressing challenges in the rapidly evolving digital and competition policy landscape. This analysis was conducted independently and received no funding. It reflects solely the views of its author, not those of its clients, which include Alphabet.

This paper is part of our Digital Competition Hub (https://www.digital-competition.com/digitalcompetitionregime). We provide research on the design, implementation, and enforcement of digital competition regimes worldwide.

Contact us for membership, service, or press inquiries.

Dr. Christophe Carugati

Dr. Christophe Carugati (christophe.carugati@digital-competition.com) is the founder of Digital Competition. He is a renowned and passionate expert on digital and competition issues with a strong reputation for doing impartial, high-quality research. After his PhD in law and economics on Big Data and Competition Law, he is an ex-affiliate fellow at the economic think-tank Bruegel and an ex-lecturer in competition law and economics at Lille University