European Law Blog, 2026 · ISSN 2950-1970
Published: 21 October 2026
DATA PROTECTION AND DIGITAL GOVERNANCE

Overlapping GDPR and DMA Competences to Assess Anonymisation: Sincere Cooperation in the Commission's Google Search Specification Decision

Paweł Hajduk and Paul De Hert
Paweł Hajduk — Cardinal Stefan Wyszyński University in Warsaw · Paul De Hert — Vrije Universiteit Brussel / Tilburg University

On 16 July 2026, the Commission adopted a decision specifying Alphabet's obligations to share Google Search data under Article 6(11) of the Digital Markets Act (DMA). In specifying those obligations under Article 8(2) DMA, the Commission prescribes safeguards and then relies on them to conclude that end users' data are anonymous for recipients. It thereby shapes the circumstances on which GDPR protection depends, although formal supervisory competences remain with data protection authorities (DPAs). The Commission intervened because it considered Alphabet's existing offer ineffective, with almost no take-up despite interest from competing search engines (recitals 26-27).

Article 6(11) requires access to ranking, query, click and view data on fair, reasonable and non-discriminatory terms, with personal query, click and view data to be anonymised. The decision combines technical alterations of search data with contractual and organisational safeguards, including prohibitions on re-identification and linkage and independent assurance audits (Annex, paras 28-36, 48-50 and 68-86). It documents *ex ante* consultation with the European Data Protection Board (EDPB), but leaves open how that consultation relates to the mandate of national DPAs competent for the particular processing under the GDPR. The central question is what happens if a competent DPA finds the prescribed safeguards insufficient even when implemented as required.

Anonymisation and the reach of GDPR supervision

The decision should not be reduced to a choice between a GDPR standard of anonymisation and a separate, narrower DMA standard.Article 6(11) DMA requires Alphabet to anonymise the search data it shares with competing search engines so that those recipients cannot identify the users who generated them, taking into account the means reasonably likely to be used. The GDPR provides the test for deciding whether those users remain identifiable. Article 2(25) DMA adopts the GDPR's definition of personal data, and the draft Joint Commission–EDPB Guidelines apply that definition to anonymisation under the DMA (paras 178-181). Alphabet should therefore choose methods that keep the search data useful while preventing recipients from identifying those users.

The narrower scope of the DMA requirement concerns whose identity must be protected. A search query may contain personal data about both the person making the search and someone named in it. Under the draft Joint Guidelines and the Commission's decision, the anonymisation obligation concerns the person making the search. Information about the person named in the query may remain personal data, and its sharing and further processing remain subject to the GDPR (Guidelines, para. 183; decision, recitals 551 and 800). This distinction is consistent with the Court's reasoning in *EDPS v SRB*, C-413/23 P. The Court held that pseudonymised information need not be personal data for every recipient. Effective safeguards may prevent identification, provided the recipient cannot lift them and has no other means reasonably likely to be used to identify the individual (paras 75-87). Relying on that reasoning, the Commission assesses identifiability from the perspective of eligible search engines (recitals 550-552). Data may therefore remain personal for Alphabet while being anonymous for a recipient. Alphabet's own processing remains subject to the GDPR. In *EDPS v SRB*, the controller's information duty was assessed at collection, before transfer, irrespective of whether the data would subsequently be personal from the recipient's perspective (paras 110-115). Here, the GDPR continues to govern Alphabet's processing undertaken to produce the dataset, as well as the sharing and further processing of personal data concerning other individuals in queries or results (recitals 551 and 800).

This recipient-specific assessment also reflects the contextual nature of anonymity. The EDPB's Guidelines 02/2026 on Anonymisation, adopted for public consultation on 7 July 2026, set out three criteria: No Record Isolation, No Linkage and No Inference. Failure to meet one

requires further analysis rather than automatically establishing that the data are personal (para. 52). Technical, organisational and contractual controls are assessed against actual identification capabilities (para. 90). The Commission's combination of safeguards, periodic review and reopening mechanisms reflects this approach, without establishing that its measures achieve anonymity in every processing context.

The Commission's assessment addresses whether recipients' processing of end users' data falls within the scope of the GDPR; the decision does not, however, replace supervision by competent DPAs. Alphabet and recipient search engines must recognise their respective positions as independent controllers (Annex, paras 45-47). The decision's effect on a later supervisory assessment by the DPAs under the GDPR remains unclear. The decision also engages with legal grounds for processing; recital 797 treats the mandatory sharing of individuals other than end users as necessary under Article 6(1)(c) GDPR and the contestability objective as a substantial public interest under Article 9(2)(g) GDPR. These are the Commission's interpretations; whether particular processing satisfies all applicable conditions remains subject to assessment by competent DPAs and courts.

The Commission's framework and DPA independence

Recitals 870, 876 and 897 show how the Commission's safeguards inform its assessment of anonymity. In recital 870, the Commission relies on the legally binding technical and contractual conditions it has prescribed as means of reducing residual re-identification risks to an insignificant level. Recital 876 connects compliance with those conditions to its conclusion that data of end users are anonymous for recipients, while treating potential breaches of those contractual measures as increasing risk of identification sufficiently to make those data personal again. The Commission thus both prescribes the conditions under which search data must be shared and relies on them to assess whether recipients' processing of end users' data falls within the GDPR.

Its engagement with national DPA decisions reinforces that point. In recital 896, it distinguishes four decisions of the French, Austrian and Irish authorities by reference to processing contexts and possibilities of identification of natural persons. The Commission does not depart from those findings. Recital 897 distinguishes them by noting that they did not involve comparable technical and contractual conditions imposed by a public authority and incapable of being

modified or lifted by the parties.

This approach should be examined against the requirement of independent supervision of data protection law in Article 8(3) of the Charter of Fundamental Rights. In *Commission v Germany*, C-518/07, the Court held that supervisory authorities must remain free from direct and indirect external influence; even a risk of political influence may compromise their independent actions (paras 30 and 36). That judgment concerned state scrutiny of DPAs and does not establish that another regulator's lawful specification of safeguards infringes their independence. Nor do DPAs have exclusive authority over every matter involving personal data. The concern here is whether the Commission's assessment could constrain a DPA's ability to reach a different conclusion under the GDPR.

A competent DPA retains powers to investigate Alphabet or a recipient, assess identification capabilities and safeguard effectiveness, and examine the lawfulness of processing and the parties' actual roles. That mandate must nevertheless be read alongside Article 1(7) DMA, which prohibits national authorities from adopting decisions running counter to Commission decisions under the DMA. The DMA also requires compliance with other Union law: recital 12 DMA preserves other Union legislation, and Article 8(1) DMArequires implementation measures to comply with the GDPR.

Suppose Alphabet and a recipient search engine implement all the safeguards exactly as required by the decision, yet the competent DPA concludes that end users remain identifiable to that recipient. Which assessment then governs? Could the DPA require additional safeguards or restrict the processing without adopting a decision that runs counter to the Commission's decision under Article 1(7) DMA? The disagreement would concern the sufficiency of the prescribed framework despite full compliance. Article 1(7), read alongside the requirement of GDPR compliance in Article 8(1), does not expressly settle how that disagreement should be resolved. This is the potential constraint on independent supervision that requires clarification.

Still, the decision preserves an operational role for DPAs. Alphabet must notify the lead supervisory authority of suspensions of access, restorations and terminations, and temporarily preserve data where a DPA is acting (Annex, paras 160, 166-167 and 173-175). That is the lead authority for the recipient search engine's processing (recital 1342). These safeguards facilitate subsequent supervision and collaboration between authorities, but do not demonstrate *ex ante*

involvement by a competent national DPA.

Cooperation and the visibility of independent supervision

In *Meta Platforms and Others*, C-252/21, the *Bundeskartellamt*, a national competition authority, assessed GDPR compliance when examining an abuse of dominance under Article 102 TFEU. The Court permitted that incidental assessment while requiring sincere cooperation with competent supervisory authorities (paras 47-59). The competition authority must ascertain whether a competent DPA has addressed the same or similar conduct and may not depart from such a decision. Consultation is required where it doubts the meaning or scope of that decision, where the conduct is under DPA examination, or where its own preliminary assessment indicates a GDPR infringement. It may continue if the DPA does not respond or object within a reasonable period.

Although *Meta* concerned a national competition authority, the draft Joint Guidelines make the connection to DMA enforcement explicit. They identify cooperation between the Commission, the EDPB and national DPAs as required by Article 4(3) TEU. Consultation is necessary where examining DMA compliance also entails examining consistency with the GDPR (paras 215-217). Paragraph 218 identifies the relevant lead supervisory authority as the Commission's interlocutor in principle, where applicable, and envisages cooperation with concerned authorities under the GDPR. Although still draft, these Guidelines provide a point of reference for assessing the relationship between the Commission's mandate under the DMA and GDPR supervision.

Measured against that reference point, the decision shows how the Commission consulted the EDPB. Recital 95 records discussions on 6 February, 18 March and 30 March 2026, written comments on 5 May, and discussion of revised measures on 15 June. The EDPB's input affected the final decision. The Commission attributes targeted pre-deployment testing to the EDPB's identification of a risk that models trained or fine-tuned on the dataset could reproduce information in their outputs (recitals 856-858). It also cites the EDPB's comments concerning technical safeguards (recital 618).

The record also shows that the Commission did not adopt every safeguard suggested by the EDPB. The EDPB encouraged it to assess additional transformations of click data, including URL

shortening or noise. The Commission declined these measures because of their effects on data quality and usefulness (recital 689). It relied on alternative safeguards in recital 690. This records a difference over the choice of measures, without establishing that the EDPB regarded the final framework as insufficient.

The EDPB has its own advisory mandate. It acts independently under Article 69 GDPR and advises the Commission on personal data protection under Article 70(1)(b). Collective advice by the EDPB nevertheless performs a different function from supervision of particular processing activities by a national authority exercising its own powers under the GDPR. The decision does not identify whether a competent national authority contributed in its supervisory capacity or explain how the relevant cooperation mechanisms were engaged. The omission does not mean that a competent DPA was excluded or that consultation was legally inadequate, but it leaves unexplained how collective advice related to supervision of the particular processing.

Recital 85 adds a procedural transparency issue. The Commission refused Alphabet access to its EDPB meeting minutes under Article 34(4) DMA, treating them as internal documents and inter-authority correspondence. It relied on the EDPB's composition of competent national authorities and invoked good administration and sincere cooperation when defending confidential technical deliberations. This is the decision's only express reference to sincere cooperation. The EDPB's written comments of 5 May were, however, shared with Alphabet on 6 May.

The refusal need not infringe Alphabet's procedural rights, but it limits scrutiny of the administrative actions beyond what the published account offers. The relevant question for our argument is how that consultation relates to independent supervision of the particular processing. Recital 689 offers an example of a proposal and the reasons for rejecting it. The published reasoning should identify the capacities in which authorities contributed. This would improve institutional accountability without requiring disclosure of every deliberation. This is our proposal about the visibility of independent supervision, not a disclosure duty derived from Article 34(4).

Does the Commission decide when the GDPR applies? The decision does not transfer GDPR supervisory competence to the Commission. It shows, however, how the exercise of DMA

powers can affect the conditions on which data protection depends. The difficulty is particularly visible where the Commission relies on its own safeguards to establish anonymity, and an independent DPA might consider those safeguards insufficient. Consultation with the EDPB by the Commission is a substantial counterweight to that concern but does not resolve it entirely.

As our earlier work on cross-regime enforcement argues, overlap can improve institutional capacity even as it creates difficulties for legal certainty. The same conduct engages different regulatory objectives, and cooperation can combine expertise and resources and improve the effectiveness of overall protection without reallocating formal competences. There is also a word of caution. In our discussion of power accumulation in the EU digital *acquis*, we argued that formal competences do not exhaust the distribution of *de facto* power. The Google Search decision shows one mechanism through which such influence could develop. Whether repeated decisions of this kind would constrain DPAs' independence remains a prospective risk. Sincere cooperation, given practical effect through further EU legislation or authorities' initiatives within the existing legal framework, should clarify the room for independent supervisory assessment and the procedure for resolving potential disagreements and conflicts of competences.

AVAILABLE AT

https://europeanlawblog.eu/overlapping-gdpr-and-dma-competences-to-assess-anonymisation/

CC BY-SA 4.0