BEUC The European Consumer Organisation

The Consumer Voice in Europe

Guidelines on the interplay between the DMA and the GDPR

December 2025

Why it matters to consumers

The Digital Markets Act (DMA) seeks to rebalance digital market by limiting the market power of large tech platforms, fostering competition, and giving consumers greater choice. The General Data Protection Regulation (GDPR) aims to protect personal data and to ensure that people remain in control of their data. Since designated gatekeepers under the DMA may also act as controllers of personal data under the GDPR, both regulations can apply to the same processing activities carried out a company. The EU consultation on the interplay between the DMA and the GDPR aims to ensure consistent protection of consumers' rights, harmonised application of European rules, and the promotion of a fairer, more transparent digital environment.

Published | 19 December 2025
Contact | competition@beuc.eu
Reference | BEUC-X-2025-118
Document coordinator | Michele Buonanno
Credit | Photo by Mudassir Ali from Pexels

The European Consumer Organisation (BEUC) is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 40 independent national consumer organisations from over 30 European countries. Together with our members, we inform EU policies to improve people's lives in a sustainable and fair economy and society.

BEUC, The European Consumer Organisation
Bureau Européen des Unions de Consommateurs AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

Introduction

In October 2025, the European Commission and the European Data Protection Board (EDPB) launched a public consultation to gather feedback on draft guidelines on the interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). BEUC welcomes this initiative as an essential step to clarify interconnections between the DMA and GDPR.

There is an urgent need to increase cooperation between authorities for an effective implementation and enforcement of the EU digital rulebook[1] (e.g. GDPR, DMA, Digital Services Act, the Unfair Commercial Practices Directive, AI Act). While the DMA foresees cooperation between authorities in the framework of its High-Level Expert Group[2], we need clarity on how laws are interpreted and applied. This is essential to ensure consistency and provide greater legal clarity for stakeholders and consumers across borders.[3]

BEUC supports several points in the draft guidelines, notably:

- The need to establish a clear connection between the GDPR and the DMA and clarifying that, whilst different in purpose, these two laws are **complementary**.[4]

- Gatekeepers must **demonstrate compliance** with the DMA by implementing measures that protect the integrity of their hardware or operating system, and by keeping an exhaustive list of the measures put in place and the rationale thereof.

- Recognizing the existence of a **system of cooperation** between authorities to ensure coherent enforcement of data-related obligations where different regulatory frameworks intersect.

That said, additional points may require consideration in the guidelines.

Consent under DMA is needed for specific data processing

Gatekeepers are considered processors of personal data under the DMA and are

[1] For instance, BEUC analysed Meta's pay or consent mechanism from a UCPD, DMA and GDPR perspectives *(www.beuc.eu/letters/concerns-about-metas-amended-pay-or-consent-subscription-model-and-lack-compliance-ucpd)*.
In several enforcement actions, BEUC informed several enforcement authorities (ERGA, EDPB, CPC) as pieces of EU legislation came into play (see for instance our work on TikTok*: www.beuc.eu/enforcement/tiktok-without-filters#documents*).
[2] Art.40 DMA
[3] On the need of a better cross disciplinary cooperation, see *Modernising consumer protection int the EU (here*-(November 2025) and *BEUC's recommendations on harmonising cross-border procedural matters in the* GDPR **(***here*-2023).
[4] This reading is in line with Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms In that position, the EDPB had already clarified that all the principles set forth by the data protection law must be respected, in general (para 57-65), and with specific regard to the consent requirement (67-69).

simultaneously data controllers under the GDPR. The interplay between the two regulations is therefore inevitable. When this occurs, the DMA and the GDPR should be interpreted in a compatible and consistent manner.

The DMA prohibits four types of personal data processing **unless** the user consents to it. The only legal basis allowing this processing is therefore consent, and not the wider range of legal bases included in the GDPR. In these specific occasions, the DMA **specifies** the GDPR and limits the number of legal bases available for a certain type of processing.

This dynamic is very similar to the one between the e-Privacy Directive and the GDPR. The e-Privacy Directive restricts the number of legal bases available, requiring service providers to request (and obtain) consent to store and access cookies. As such, this provision in the e-Privacy Directive takes precedence over the GDPR.[5]

The EDPB has already noted "*that certain provisions of the Digital Markets Act ('DMA'), such as Art. 5(2), lay down **specific rules** for so-called 'gatekeepers' processing personal data*" (emphasis added).[6]

BEUC recommends that the guidelines clearly mention the relation lex generalis/specialis existing between Art. 5(2) DMA and Art. 6 GDPR. The guidelines should provide examples of the different interactions. This would enhance legal certainty and foster more consistent enforcement of both the DMA and GDPR.[7]

The DMA and GDPR complement each other in specific cases

The DMA refers to the GDPR for the definition of consent. The EDPB has already clarified what consent means in the context of Meta's "Pay-or-Consent" subscription model.[8] As BEUC has consistently stressed[9], consent under the GDPR must be freely given, specific, informed and unambiguous. These are the clear boundaries within which Article 5(2) of the DMA consent must operate.

BEUC is therefore sceptical about the overall validity of the Pay-or-Consent model used by gatekeepers. There is an **inherent incompatibility** between the implicit notion of consent under the GDPR and the consent dynamics the Pay-or-Consent models

[5] EDPB, 12 March 2019, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*
[6] EDPB, 17 April 2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, para. 46.
[7] For instance, authorities and stakeholders (both businesses and civil society) could refer to the practice and case law developed for the GDPR when dealing with a DMA data-related obligation, whose interpretation has not yet been clarified in the context of the DMA.
[8] EDPB, 17 April 2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.
[9] For example, see BEUC Comments on EDPB Guidelines 2/2019 on the processing of data under Article 6(1)(b) GDPR in the context of the provision of online services.

suggest.[10] The structural asymmetry of control and information between platforms and users makes a valid GDPR consent hardly imaginable.[11]

This conclusion follows directly from Art. 7 GDPR, which lays down strict conditions for valid consent. Furthermore, the GDPR emphasises that users must have a genuine choice and should not face any negative consequences if they refuse consent. Consent is invalid when there is a clear imbalance between the one controlling the data and the user and when access to a service is tied to data processing that is not necessary. This reflects the dependency and lock-in effects consumers experience with gatekeepers.

The DMA confirms these elements, as the regulation prohibits behaviour limiting the protections provided by Art. 5 DMA. Art. 13(6) DMA is even clearer as it highlights that a gatekeeper's behaviour must not make it harder for consumers to exercise their **rights** or make their own **choices**. Additionally, a gatekeeper should offer those choices in a neutral way.

In short, the DMA works alongside the GDPR,[12] and rejects the idea of undermining the consumer's autonomy to make their own choices. Consumers do not have autonomy – or it is severely diminished – if all the choices are not presented in a neutral manner. This is the case, for instance, when the gatekeeper gives more importance to some options over others, or when they are presented in different moments of the user's experience.13

BEUC suggests that greater references are made to these elements and to its previous guidance to ensure a consistent interpretation of the two regulations and provide stakeholders with useful tools for their compliance. Some concrete examples may also be added to increase clarity.

The notion of service provided together with or in support of a CPS

The prohibition set out in Art. 5(2) DMA applies to cross-use/the combination of personal data between a Core Platform Service (CPS) and another CPS or another service provided by the gatekeeper. Cross-use/combination of personal data between a CPS and a "*service provided together with or in support of a CPS*" is not covered by Art. 5(2) DMA.

10 This is especially true for the "freely given" aspect of consent. The EDPB' has clarified that to satisfy such requirement, the data subject must not incur in any "*detriment*". In particular, "*The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent*." EDPB, 4 May 2020, *Guidelines 05/2020 on consent under Regulation 2016/679*, para. 46-47.

11 EDPB, 17 April 2024, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, para. 182.

12 Recital (12) DMA.

13 This is particularly important if the controller narrows down the data subject's range of choices (e.g. by not providing a Free Alternative Without Behavioural Advertising, as described below in Section 4.2.1.1) or makes choices which may risk unduly influencing the data subject's choice (e.g. by charging a fee that is such to effectively inhibit data subjects from making a free choice). EDPB, *Corrigendum to EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, para. 60.

On this point, the Draft Joint Guidelines specify that for a relevant service to be qualified, it must have a "*close functional interconnection*" with the CPS or other gatekeeper service and provide a series of examples. BEUC welcomes the clarification of the legal text based on the "*close functional interconnection*" and acknowledges, as the European Commission and the EDPB did, that this point could be the opportunity to clarify certain case uses.

However, BEUC recommends clarifying whether AI should be considered as a "*service provided together with or in support of a CPS*". In addition, AI technology might need to be added to the list of examples in paragraph 70 of the draft Guidelines. This would clarify whether the introduction of AI on gatekeepers' platforms should be considered as a service provided together with a CPS, and as such, not covered by Art. 5(2) DMA – or as another service, which would trigger the application of Art. 5(2) DMA.

This is particularly relevant now that gatekeepers tend to argue that AI is a technology embedded in their CPS.[14] BEUC argues that, based on the differences in the function of technology, AI should be considered as a separate service.[15]

Sincere cooperation between authorities

The Draft Joint Guidelines comment on a system of consultations between authorities competent for monitoring compliance with different legal frameworks.

In practice, the Commission or the relevant national lead supervisory authority should examine whether the gatekeeper's conduct is consistent with either the GDPR or the DMA.[16] However, BEUC highlights that cooperation does not mean control. Data protection authorities should be free from any external control, including from the European Commission.

BEUC supports this suggestion: a system as that strengthens sincere cooperation between authorities as enshrined in Art. 4(3) TFEU. EU authorities and Member States, including their administrative bodies, must support each other and fulfil their respective obligations under national and EU law. In doing so, they must refrain from any measure that could jeopardise the European Union's objectives.[17]

Enhancing interinstitutional cooperation is key to navigating a multi-level enforcement landscape, and the Guidelines on the interplay between the GDPR and the DMA provide an opportunity to clarify how authorities can cooperate more effectively in practice.

[14] See Meta's DMA Compliance Workshop held on 3rd July 2025, available here.
[15] See BEUC's submission to the European Commission on Meta AI technology, paragraph 3.2.1, available here.
16 Paragraph 217, Draft Joint Guidelines on the Interplay between DMA and GDPR.
[17] See, to that effect, judgments of 7 November 2013, UPC Nederland, C-518/11, EU:C:2013:709, paragraph 59, and of 1 August 2022, Sea Watch, C-14/21 and C-15/21, EU:C:2022:604, paragraph 156. Also, Case C-252/21, *Meta Platforms and others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, paragraph 53.

The cooperation is not only for enforcement purposes. For instance, the different authorities should cooperate when drafting guidance, such as Guidelines or Opinions. Finally, BEUC suggests entrusting the High-Level Group set up in Art. 40(5)(b) DMA to monitor the respect of these obligations.[18]

--

[18] This possibility is only briefly discussed at Point 220 of the Draft Joint Guidelines.