Consultation on joint guidelines on the interplay between DMA and GDPR

CCIA Europe response

December 2025

The Computer and Communications Industry Association (CCIA Europe) welcomes the opportunity to participate in the European Commission and European Data Protection Board's (EDPB) public consultation on the draft joint guidelines on the interplay between Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR), (Draft Guidelines).

To inform the joint work of the EDPB and the European Commission, CCIA Europe would like to respectfully offer the following set of recommendations.

I. Ensure coherence between GDPR and DMA enforcement

CCIA Europe emphasizes that coherence between the DMA and the GDPR, as well as the protection of the right to privacy, are essential for legal certainty, innovation, and strong user protection.

Recommendations:

1. Allow vetting of third parties in the interpretation of Article 6(9)
2. Allow GDPR-standards of anonymisation in the interpretation of Article 6(11)

II. Clarify legislative interplay, while avoiding regulatory overreach

CCIA Europe emphasizes that the Draft Guidelines should be focused on clarifying interpretative doubts and the interplay of the legislations, and not result in the creation of new obligations not foreseen by the letter of the law.

Recommendations:

1. Carefully balance consent with end-user experience in the interpretation of Article 5(2)
2. Avoid creating new obligations in the interpretation of Article 6(9) and 6(10)
3. Avoid incomplete and contradicting interpretations of the DMA and the GDPR

Introduction

CCIA Europe welcomes the Draft Guidelines issued by the European Commission and the European Data Protection Board (EDPB)[1], recognising them as a valuable step toward legal certainty, reduced conflicts of law, and an overall clearer interaction between the DMA and the GDPR.

However, CCIA Europe remains concerned that the Draft Guidelines appear to, in some instances, subordinate the right to privacy to the DMA enforcement, and, in the effort of clarifying their interplay, introduce new requirements, which go beyond what is provided for by the DMA and GDPR.

Against this backdrop, we offer the following recommendations and respectfully note that the approach of the Draft Guidelines merits reconsideration. The Draft Guidelines should uphold legal certainty, operational feasibility, and the distinct objectives of both the DMA and the GDPR. They should focus on clarifying existing law, avoid unintended extensions of regulatory obligations, and contribute to the EU's simplification efforts.

I. Ensure coherence between GDPR and DMA enforcement

CCIA Europe emphasizes that coherence between the DMA and the GDPR, as well as the protection of the right to privacy, are essential for legal certainty, innovation, and strong user protection.

1. Allow vetting of third parties in the interpretation of Article 6(9)

CCIA Europe cautions that the Draft Guidelines, in their current form, undermine efforts to safeguard the privacy of EU users, to the benefit of DMA enforcement.

The Draft Guidelines seem to subordinate the fundamental right to data protection to the DMA's portability obligation, without clear benefits for consumers or contestability, in addition to introducing tensions with similar provisions in the Data Act.

For example, the Draft Guidelines seem to disincentivise vetting of third parties by gatekeepers (paragraphs 125 - 135) as if checks and warnings could be considered as dark patterns or measures meant to discourage users from porting data. In CCIA Europe's view, on the contrary, designated companies should be allowed to conduct proportionate pre-transfer safety and security checks on third-party data requesters, and to provide appropriate risk disclosures. Discouraging such practices weakens essential protections against malicious actors. Indeed, these checks are necessary not only to meet GDPR obligations but also to protect customers from potential harm, particularly considering that many third-party requesters[2] lack basic security safeguards or provide inconsistent information about their data-protection practices. A reasonable level of review by designated companies is therefore appropriate.

[1]Draft Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, 09 October 2025, available here.
[2] Kluwer Competition Law Blog, Amazon's Second DMA Compliance Workshop – The Power of No: Where the Balance Should Land, 24 June 2025, available here.

Moreover, the Draft Guidelines' interpretation[3] that the obligation to port data under Article 6(9) DMA operates independently of GDPR compliance directly conflicts with the approach taken in the Data Act. Indeed, the Data Act explicitly preserves GDPR primacy under Article 1(5), whereas in this case GDPR would be overridden by DMA compliance. The Commission's own Data Act FAQs[4] further confirm that, in data-sharing arrangements between controllers, each party must demonstrate GDPR compliance under the accountability principle. By departing from this framework in the DMA context, the Draft Guidelines risk creating an unjustified dual standard of privacy protection, in which a user's personal data receives different levels of protection depending on which EU instrument governs the sharing.

In a similar vein, with respect to Article 6(4) on alternative distribution, the Draft Guidelines should acknowledge that designated companies can differentiate their platforms based on different criteria, such as, for example, user privacy and data protection frameworks. This differentiation can arguably be seen as a competitive mechanism among different companies: for example, recent survey data[5] show how user and developer safety are critical factors in evaluating app stores for developers, with 92% of respondents mentioning an app store's approach to user safety and security (e.g. protecting user data, removal of malware), as well as an app store's security measures for developers (e.g., protection of IP, prevention of piracy) is important to them. Gatekeepers whose platforms are defined by specific, publicly articulated privacy commitments, should be thus permitted to require equivalent adherence to these commitments from third-party app developers and alternative distribution channels, if these requirements are considered strictly necessary and objectively linked to the integrity and consistency of the gatekeeper's defined privacy framework, which forms a core basis for consumer choice.

While the DMA creates new data-sharing obligations, it explicitly preserves GDPR protections (Recitals 6, 12, 59, and Article 8(1)). We thus believe that in this respect, the Draft Guidelines should reaffirm GDPR precedence, and permit a reasonable level of review by designated companies, not discourage it.

2. Allow GDPR-standards of anonymisation in the interpretation of Article 6(11)

CCIA Europe sees an inherent tension between the requirement to share data in an *anonymised* manner, provided for in Article 6(11), and the guidance provided for in the Draft Guidelines.

In particular, providing access to anonymised search data requires an extremely high standard of anonymisation to protect user privacy effectively. Such high bar and requirement clashes with the mandate in paragraph 180 of the Draft Guidelines to adopt an anonymisation method that "preserves the most quality and usefulness of the data for the third party undertaking requesting access 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".

[3] Draft Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, paragraphs 105 – 106, 9 October 2025, available here.
[4] European Commission, Frequently Asked Questions about the Data Act, 6 September 2024, available here.
[5] MTM, EU Developer Attitudes Towards App Stores, July 2025, available here.

CCIA Europe believes that in this case, the right to privacy shall be given primacy. If this is not the case, the Guidelines risks leading to situations in which the obligations resting on gatekeepers are conflicting, i.e. personal data cannot be anonymized and yet must be shared.

More specifically, CCIA Europe cautions against the Draft Guidelines' reliance on the SRB judgment[6] to mandate re-identification risks being assessed against "unintended recipients." Such an interpretation risks misapplying a judgment concerning publication of public data to a context of controlled business-to-business (B2B) transmission. Requiring gatekeepers to account for unknown third parties would render the Guidelines not only highly burdensome but also ineffective.

We thus suggest that the Draft Guidelines explicitly state that any implementation of Article 6(11) is conditional on robust, state-of-the-art security and full, demonstrable compliance with the GDPR's high anonymization standard.

II. Clarify legislative interplay, while avoiding regulatory overreach

CCIA Europe emphasizes that the Draft Guidelines should be focused on clarifying interpretative doubts and the interplay of the legislations, and not result in the creation of new obligations not foreseen by the letter of the law..

1. Carefully balance consent with end-user experience in the interpretation of Article 5(2)

While CCIA Europe agrees with the goal of ensuring that consumers are aware of how their data is being used, and for what purposes, we believe that the enforcement of the DMA, based on the current Draft Guidelines, will not achieve the ultimate objective of increasing contestability, but will, on the contrary, result in an overly burdensome consent experience, exacerbating and further negatively impacting the user experience in the use of gatekeepers' services.

Recent consumer surveys indicate that the DMA is generating more friction than benefits for users.[7] Reports show that most Europeans find their online experience worse than before early 2024: two-thirds say they now spend more time searching for relevant content, and 59% bypass DMA-mandated choice screens by going directly through apps. Early implementation data also shows significant consumer frustration.[8] Thirty-nine percent of users report needing more steps for tasks that were previously simple, and roughly one-third describe their digital experience as "less seamless and more confusing."[9] These trends reflect well-documented consent fatigue: excessive or poorly timed prompts do not improve informed decision-making but instead lead to confusion, arbitrary choices, and a diminished user experience. This outcome is counterproductive and runs against the GDPR's core principles of clarity and user-friendliness. The Commission itself noted similar

[6] Judgment of the Court of Justice of 4 September 2025, EDPS v. SRB, paragraph 55, available here.
[7] Nextrade economics, *Impact of the Digital Markets Act (DMA) on Consumers across the European Union,* September 2025, available here.
[8] ECIPE, *What About Us? Consumer Response to the Digital Markets Act*, October 2025, available here.
[9] *Ibidem.*

concerns in its September 2025 work on ePrivacy, mentioning that users being confronted with repetitive consent requests and opaque cookie banners in practice, undermines genuinely informed choice.

Beyond being ill-suited for improving consumer understanding, the Draft Guidelines exceed the scope of the DMA: indeed, while the DMA regulates data sharing between services, the Draft Guidelines go beyond the DMA's framework, transforming this into a purpose-specific consent system (paragraphs 31 - 63). Requiring opt-in consent for service development (paragraph 31) is disproportionate to the objective of Article 5(2), as it risks hindering innovation without delivering corresponding contestability, nor privacy benefits, particularly where data-minimising techniques already exist and additional per-service prompts would exacerbate well-documented consent fatigue. The measure risks user confusion, potentially leading users to conflate distinct legal decisions and misunderstanding the implications of each specific choice. Users may fail to differentiate between choices governed by the DMA, relating to cross-use and data sharing, and those governed by the GDPR,. This overreach also raises practical concerns previously acknowledged by the EDPB, which noted in its letter to the Commission on the Cookie Pledge initiative that overly technical or lengthy explanations make informed choice complex, burdensome, and ineffective.[10]

Similarly, mandating explicit consent for special categories of personal data in the context of Article 5(2) introduces obligations not foreseen in the DMA itself. While safeguarding sensitive data remains essential, existing rules under the GDPR are comprehensive enough, and adding this requirement to the DMA framework would warrant careful consideration to ensure it addresses a genuine regulatory gap and does not introduce further complexity without clear benefit for users.

Overall, the Draft Guidelines should aim at enhancing consumer experience based on transparency and information instead of unnecessary friction. The Guidelines should take a proportional approach, carefully balancing users' right to consent, but at the same time allowing companies to innovate on how they offer services, without introducing disruptive or unnecessary choice interface.

2. Avoid creating new obligations in the interpretation of Article 6(9) and 6(10)

In relation to Article 6(9) and Article 6(10) DMA, CCIA Europe maintains that the Draft Guidelines appear to go beyond the letter of the law, requiring solutions which appear technically unworkable in relation to multiple provisions.

1. **Extension to "on-device data" and "generated data":**

In both paragraphs 107 - 111 in relation to Article 6(9), and paragraphs 147 - 154 in relation to Article 6(10), the Draft Guidelines extend the reach and type of data which gatekeepers are obliged to port, both in relation to end-users, and in relation to business users. Indeed, the sections broaden the scope of the articles to "on-device" data, "generated data" (for Article 6(9)), as well as to general technical data such as IP addresses, and wider end-user platform behaviour, in the case of Article 6(10). These

[10] EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, 19 December 2023, available here.

extensions seem unfounded in the DMA, and raise feasibility, privacy and security concerns, and are difficult to reconcile with the Draft Guidelines' own position that data portability should not result in gatekeepers obtaining additional on-device data.

Including on-device data introduces substantial technical and practical challenges, particularly where the gatekeeper does not access or process such data. For example, requiring portability for on-device data could introduce major technical challenges and security vulnerabilities, potentially necessitating new and complex transfer mechanisms outside existing secure cloud infrastructures. Moreover, the inclusion of personal data relating to other individuals within a user's portability request raises additional privacy concerns and creates practical difficulties in separating data or obtaining the necessary consents.

2. **Gatekeepers' obligation to provide a dashboard listing all recipients of personal data concerning third parties other than the requesting user**

The prescriptive provision in paragraph 113 does not seem to have a basis in the DMA, and would impose an operationally unworkable requirement, as companies would be expected to track, maintain, and disclose all indirect data transmissions involving third-party personal data that may be incidentally captured in portability requests. Designing and maintaining such a system would be extremely complex, if not impossible in practice, given the difficulty of identifying, segregating, and documenting every downstream disclosure involving individuals who are not the requesting user. It may also require the gatekeeper to process additional personal data (tracking all recipients) solely for the purpose of this dashboard, creating a direct conflict with the principle of data minimisation.

3. **Continuous and real-time access:**

In paragraphs 120 – 124 in relation to Article 6(9), and paragraphs 165 - 170 in relation to Article 6(10), the Draft Guidelines interpret the DMA's provisions in Articles 6(9) and 6(10) of "continuous and real-time access to data" as indefinite and perpetual access. In CCIA Europe's view, such interpretation is not supported by the DMA text and does not take into consideration key security and privacy risks.

Indeed, continuous, long-term access is a known driver of major data breaches because accounts or applications may retain permissions they no longer need, enabling compromise, persistent access, and lateral movement. Also, revoking such access in real time during incidents is also difficult. A more practical interpretation would prioritise efficient, periodic, or user-initiated transfers, or API access with reasonable duration limits. Article 6(10) should instead permit flexible, user-configured access durations, including one-time access, fixed periods, or access "until withdrawn" by the end user. Gatekeepers should be able to apply reasonable time limits (e.g., one year) to mitigate risks such as fraud, account takeover, and accumulated permissions that attackers can exploit. This is particularly important given that many third-party requesters lack robust security controls, offer limited transparency about their practices, or are located in jurisdictions with weaker data-protection standards. Without appropriate duration limits, continuous access could allow malicious actors to aggregate and misuse personal data over extended periods.

4. Online choice architecture, especially in relation to nudging

In paragraphs 125-127 in relation to Article 6(9), and paragraphs 171-174 in relation to Article 6(10), the Draft Guidelines require portability options to be presented neutrally and without nudging, but provide no clarity on the distinction between improper nudging and legitimate risk disclosure. This ambiguity risks treating factual security warnings, such as informing users that certain third parties lack basic security and privacy safeguards, as prohibited nudging. The Draft Guidelines should explicitly recognise that such disclosures are not nudges but essential elements of informed user choice and required under the GDPR's transparency obligations.

3. Avoid incomplete and contradicting interpretations of the DMA and the GDPR

CCIA Europe considers that the Draft Guidelines in their current form lack analysis of certain important provisions, and risk creating further contradictions between established GDPR notions and the DMA.

For example, the Draft Guidelines make a key omission by not even considering the security, privacy risks and GDPR implications from DMA Article 6(7). Given that this article represents a crucial point of overlap between the DMA and the GDPR, the Draft Guidelines should stress the need for the EDPB and national data protection authorities to be involved when gatekeepers' compliance with Article 6(7) risks undermining users' privacy rights and the GDPR. Indeed, the Draft Guidelines could be the right opportunity for the Commission and the EDPB to clarify how the integrity exception in Article 6(7) should be properly read in light of the GDPR.

In relation to confusing provisions, CCIA Europe notes conflicting messages around user consent, fewer personalised options, and GDPR compliance (paragraphs 23 - 35 of the Draft Guidelines, and Article 5(2) DMA). Indeed, under the DMA, a gatekeeper may offer a less personalised but otherwise equivalent version of its service to non-consenting users, and may reduce or disable certain features when such degradation is technically unavoidable due to the absence of personal data, provided the user is clearly informed of this. However, under the GDPR, any negative consequence linked to a refusal of consent can be considered a detriment, which risks rendering the consent invalid as not "freely given." This means that even technically unavoidable service degradation permitted under the DMA could simultaneously be viewed as unlawful under the GDPR. As a result, gatekeepers may be placed in an impossible position: complying with the DMA's requirement to acknowledge and explain unavoidable degradation could lead to a violation of the GDPR's strict prohibition on detriment associated with withholding consent. On this note, CJEU case law confirms that the notion of detriment requires actual coercion, and can therefore not be applicable just because a gatekeeper is requesting consent.[11] CCIA Europe thus stresses that the Guidelines should be consistent with CJEU case law.

Further, the Draft Guidelines could give greater consideration to the significant adjustments that services must undertake when required to modify their underlying business models. At this stage, allowing more flexibility would be warranted, particularly in light of the recent

[11] For example, please see: F v Bevándorlási ruling, Case C-564/18, available here, and Opinion of Advocate General Sharpston in Schecke, available here.

CJEU judgment in C-252/21[12], which expressly allows any operator of any size to offer an equivalent alternative service (i.e., the service without ads) for an appropriate fee, and the ongoing debates reflected in the EDPB's Opinion 8/2024, which itself remains subject to judicial scrutiny.[13]

Finally, there appears to be confusion between paragraph 69 and 72–75 of the Draft Guidelines, in relation to the type of consent required for cross use of personal data (Article 5(2)c DMA). Indeed, paragraph 69 of the Draft Guidelines applies a strict necessity test, mentioning that "only personal data that is *strictly necessary* to provide such interconnected functionality, [...], can be used without triggering the requirement to gather consent". On the other hand, paragraphs 72–75 of the Draft Guidelines allow for cross use of personal data without satisfying the DMA's "*strict necessity*" condition, when GDPR based legal grounds are met, notably legitimate interest and the performance of a contract, thus allowing for cross use of personal data in a wider set of circumstances, including certain advertising-related processing. However, the guidelines do not explain when gatekeepers must adhere to the DMA's narrow "strictly necessary" condition or when they can rely on the more permissive GDPR grounds for processing without consent. Without clearer guidance on how these standards interact, gatekeepers may face difficulty determining the lawful basis for cross-use of personal data and risk inconsistent compliance outcomes.

Conclusion

CCIA Europe welcomes the opportunity to provide feedback on the joint Draft Guidelines concerning the interplay between the DMA and the GDPR. We firmly believe that ensuring a coherent, legally sound, and privacy-protective implementation of both frameworks is essential to fostering trust, innovation, and effective enforcement in the digital ecosystem.

Through the recommendations outlined above, CCIA Europe aims to support the Commission and the EDPB in developing guidance that remains faithful to the letter and spirit of EU law—strengthening user rights while ensuring that compliance obligations are both practical and proportionate. We stand ready to continue engaging constructively with regulators to help ensure that the final guidelines promote robust privacy protections and legal certainty for all stakeholders.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve

[12] Judgment of the Court of Justice of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, available here.
[13] Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, available here.

understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org