bitkom

Position Paper

December 2025

Bitkom on the European Data Protection Board's and European Commission's joint guidelines on the interplay between the DMA and the GDPR

Summary

Bitkom welcomes the joint initiative of the European Commission and the European Data Protection Board to provide guidance ensuring a coherent and consistent interpretation of the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR), particularly with regard to provisions of the DMA that involve the processing of personal data by gatekeepers or refer to GDPR concepts and definitions.

A compatible and complementary interpretation of both legal frameworks is essential to guarantee a harmonised application that achieves their respective objectives: promoting contestable digital markets and safeguarding fundamental data protection rights.

While the guidelines represent an important step towards consistent enforcement, certain provisions introduce practical and legal complexities. Bitkom therefore seeks to contribute practical insights based on operational realities, with the aim of clarifying the interplay between the DMA and the GDPR and supporting legal certainty for gatekeepers, businesses and end users alike.

Data Combination and Cross-Use

Regarding the interpretation of Article 5(2) DMA, Bitkom welcomes the intention of the Guidelines to ensure meaningful user choice and compliance with GDPR principles. However, certain aspects would benefit from further clarification to ensure legal certainty, practical workability and full compliance with the prohibitions of personal data cross-use without previous user consent.

In particular, a clear distinction between consent under the DMA (limited to data combination and cross-use) and consent as a GDPR legal basis could help prevent confusion. It is operationally critical to maintain a conceptual and technical separation between the ”specific choice” regarding service models (DMA) and the legal basis for processing (GDPR). Mandating a merged consent flow risks conflating these distinct regulatory requirements. Gatekeepers should retain the flexibility to present these choices separately and at contextually appropriate moments to ensure users clearly understand the distinct scope of each decision. At the same time, it should be clear that the risk of the user leaving a CPS without having the opportunity to decide on the use of their data is considered a breach of the gatekeeper's obligations.

Moreover, the obligation to provide a free, less personalised but equivalent alternative raises questions regarding proportionality, feasibility and the preservation of viable business models, especially where personalisation constitutes a core element of service quality.

In addition, the timing of the draft Guidelines may require reconsideration, given that key elements rely on an EC decision currently under appeal and on EDPB Opinion 8/2024 (Pay or Consent), which is itself subject to judicial review. It may also be useful to consider that the CJEU ruling in C-252/21 explicitly permits service providers to offer an equivalent alternative against an appropriate fee, which could have implications for the interpretation of Article 5(2). Moreover, the introduction of a ”detriment” standard appears to go beyond existing legal requirements and may diverge from established case-law regarding consent, where reluctance to pay has not been equated with coercion.

To avoid unintended effects such as user fatigue, product degradation or consent overload, the Guidelines could acknowledge more flexible, user-friendly approaches to consent presentation that ensure compliance without undermining user experience. For instance, the Guidelines should explicitly endorse the use of multi-layered consent interfaces. As acknowledged by various national Data Protection Authorities, such designs allow users to express global preferences at the first layer while retaining access to granular, purpose-specific choices at a secondary level. This structure respects user autonomy without inducing decision fatigue through excessive clicks. A measured approach would help align the DMA’s contestability objectives with broader EU policy priorities (e.g. innovation, AI development and data-driven competitiveness) while ensuring that data protection safeguards remain fully respected.

The recently published Digital Omnibus amendments to the GDPR introduce mandatory third-party consent requirements (new Article 88b GDPR). Controllers must respect individuals' choices for processing personal data provided by automated and machine-readable means via browser settings. If consumers use automated third-party means to make their choices, it is uncertain how this will interact with Article 5(2) DMA consent obligations and requirements for designated companies. This aspect should be addressed in the guidelines at the appropriate time.

Data Portability

Bitkom supports the objective of Article 6(9) DMA to facilitate user empowerment, switching and multi-homing through enhanced data portability rights. However, certain elements of the draft Guidelines would benefit from clarification to ensure technical feasibility, legal certainty, and compliance with existing GDPR safeguards, while avoiding unintended security and privacy risks.

First, the proposed extension of portability rights to data "generated through activity", including on-device data, goes beyond the GDPR baseline under Article 20 GDPR. Clarification is warranted on the exact scope of "generated data," particularly to ensure that genuinely inferred or derived data created by gatekeepers remains outside the portability obligation, in line with GDPR interpretations. Specifically, data that is archived or stored solely in backup systems for disaster recovery should be explicitly excluded from the scope of active portability. "Unearthing" such data requires disproportionate technical intervention and contradicts the principle of data minimisation by reactivating data that is no longer in the production environment. The inclusion of on-device data raises substantial technical and cybersecurity challenges, potentially requiring the creation of entirely new transfer mechanisms that fall outside established secure cloud infrastructures. It is important to recognise that data processed exclusively on-device often relies on hardware-backed encryption or local security enclaves. Mandating the export of such data undermines the "privacy-by-design" architecture of modern devices and introduces new attack vectors by requiring decryption for transfer.

The draft Guidelines also introduce the concepts of "continuous" and "real-time" access, potentially even indefinitely, which risks conflating portability with interoperability. While APIs can support ongoing access in some use cases, truly indefinite real-time synchronization for large datasets may be operationally unworkable and significantly increase the attack surface for data breaches. A more pragmatic interpretation, focused on efficient, user-initiated periodic transfers or time-limited APIs, would better balance user rights with security and GDPR accountability obligations. Any prospective solution must also provide users with control over the duration of access, such as one-time transfers, fixed periods, or access "until withdrawn," and should underscore that continuous access raises specific security concerns. In particular, where third-party requesters lack adequate data-security safeguards, continuous access could enable malicious actors to aggregate and exploit personal data over extended periods.

Relatedly, designated companies must retain the ability to implement proportionate safety and security vetting of third-party recipients, as required under GDPR. Gatekeepers should not be prevented from applying due diligence, particularly where third parties may lack robust data protection measures. This is essential to satisfy GDPR compliance obligations and to protect users from potentially harmful actors. Similarly, gatekeepers should be permitted to notify users when data portability actions occur, as this enhances transparency and enables harm prevention.

Finally, data portability should remain focused on enabling effective switching and multi-homing, as outlined in Recital 59 DMA. Positioning "innovation" as an autonomous objective, or expanding the data scope beyond what is necessary for switching, could transform Article 6(9) into a broader data-sharing mechanism — risking a departure from the DMA's contestability objective.

In light of these concerns, Bitkom recommends that the final Guidelines provide clearer definitions of "generated data," avoid introducing new obligations regarding on-device data, maintain alignment with GDPR accountability and security principles, and support a proportionate and secure implementation framework that preserves user empowerment without imposing unworkable technical burdens or creating new risks.

Data Access for Business Users

Bitkom supports the objective of Article 6(10) DMA to enhance contestability by allowing business users to access data generated through their commercial interactions on core platform services. This provision has strong potential to enable innovation, improve data-driven services and strengthen competition. However, several aspects of the draft Guidelines may lead to operational complexity and legal uncertainty, and therefore would benefit from further clarification to ensure alignment with the DMA and existing GDPR safeguards.

First, the Guidelines appear to broaden the scope of Article 6(10) DMA beyond what is foreseen in the DMA. Article 6(10) and Recital 60 clearly refer to data provided or generated by business users, and data provided or generated by end users when engaging with those business users' products or services. However, the draft introduces additional categories, such as platform-observed data, general technical data (e.g. IP addresses), or broader end-user behaviour not directly related to business users' interactions. While it is undeniable that business users need access to sufficient data to create a level playing field, a broader interpretation could impose obligations that are not supported by the text of the DMA and dilute the core purpose of the provision. Ensuring that the scope remains linked to interaction-based data would better reflect the DMA's intent and provide legal clarity.

Second, the expectation to enable access to on-device data would pose significant technical and security challenges and does not appear to derive from the DMA. Moreover, such a requirement may overlap with the Data Act. It would therefore be helpful to clarify that on-device data falls outside the scope of Article 6(10), particularly where the gatekeeper does not process such data in the first place.

In addition, the requirement for gatekeepers to facilitate consent interfaces between business users and end users regarding access to personal data should acknowledge the practical realities of implementation. While the collection of valid consent remains the responsibility of the business user as data controller, the Guidelines could usefully recognise that uniform mechanisms may not be suitable for all core platform services, and that consent flows must be designed to avoid user confusion, friction, and fatigue. The implementation should therefore remain proportionate and flexible to ensure an intuitive user experience.

Additionally, the Guidelines bring to light an unresolved tension between the obligations of the various stakeholders involved. While gatekeepers are required to provide the technical framework for consent, this should not inadvertently shift the liability for GDPR compliance onto them. This raises critical liability issues that appear to have been overlooked: specifically, when a business user customises the consent interface (e.g., defining the processing purpose), the gatekeeper cannot be held responsible for the validity or quality of that consent. The Guidelines must explicitly clarify that gatekeepers are not required to police the regulatory compliance of independent business users, as doing so would impose an impossible operational burden.

Regarding data access duration, the DMA requires ”continuous and real-time access” but this should be interpreted as reliable access when needed, rather than indefinite or permanent access. Business users should have the ability to configure suitable durations (e.g. one-time, fixed periods, or ”until withdrawn”) with renewal options, while allowing gatekeepers to implement proportionate time limitations to mitigate security risks such as fraud, account takeover, or abuse by third parties operating in jurisdictions without adequate data protection standards. This approach would align better with GDPR safeguards and ensure that access does not inadvertently expose users to harm.

Finally, notifications and reminders about data access or consent status are essential for transparency and user awareness. Gatekeepers should retain the ability to inform users about relevant data access activities. However, Bitkom emphasises that this should be done in a clear and non-intrusive manner.

In summary, Bitkom recommends clarifying the limits of the scope of Article 6(10)—particularly regarding on-device data and general platform-observed data—while preserving flexibility in technical implementation and supporting proportionate consent and security mechanisms. This would allow business users to benefit from meaningful access to relevant data, while ensuring that the DMA’s objectives are fulfilled without imposing obligations beyond its intended remit.

Access to Anonymised Search Data

Bitkom supports the objective of Article 6(11) DMA to enhance contestability in the online search market through access to anonymised search data. It is also evident – and should not be questioned in the following – that the anonymisation of this data is the responsibility of the gatekeeper. At the same time, the Guidelines should

emphasise that robust privacy and security protections are a non-negotiable prerequisite for any data sharing. The GDPR remains fully applicable, and its high standards for anonymisation—requiring that the likelihood of re-identification is insignificant—must be respected. Simple filtering or masking techniques may be insufficient, and technical anonymisation measures should take primacy, with contractual restrictions serving only as a secondary safeguard. While ensuring the usability of anonymised data is important, privacy must prevail where there is a trade-off between utility and protection. Furthermore, the Guidelines could clarify responsibilities and risk management for third-party recipients to prevent a "security liability gap," ensuring that consumer trust is maintained and that data is handled safely throughout its lifecycle. To break this deadlock, the Guidelines should explicitly recognize that contractual safeguards (e.g., binding restrictions on re-sharing) effectively contain the data. This validation allows the risk assessment to be properly scoped to the intended recipient, aligning the DMA's contestability goals with feasible privacy compliance.

Interoperability of Core Platform Services

Bitkom supports the DMA's objective to enhance interoperability among core platform services, while ensuring that security and user trust are preserved. Interoperability obligations should fully preserve end-to-end encryption and other security guarantees across connected services. The scope of interoperability should focus on core features of the service, avoiding requirements for non-core functionalities that could compromise security. Furthermore, guidelines should reflect the DMA text, requiring technical interfaces for interoperability "upon request, and free of charge," without introducing additional obligations such as mandatory user discoverability.

Conclusion

Bitkom encourages the EDPB and the European Commission to carefully reconsider both the timing and the approach taken in the draft Guidelines. The Guidelines should uphold fundamental principles such as due process, the rule of law, and legal certainty, while ensuring operational feasibility and respecting the distinct objectives and mandates of the DMA and GDPR. Their purpose should be to clarify existing law and to avoid regulatory overreach, providing guidance that is practical, proportionate, and firmly grounded in the DMA's text. We further encourage the Commission and the EDPB to maintain high standards of accountability and diligence, ensuring that regulatory expectations are clearly articulated and actionable, even as enforcement initiatives progress.

Finally, it should be noted that the Guidelines should complement, but not substitute the role of regulatory dialogue and stakeholder engagement. The Guidelines take markedly assertive positions across a large number of obligations, while the DMA created mechanisms for dialogue and feedback. We would caution against overly specifying specific obligations without taking due account for the overall processes foreseen in the DMA and assuring the principles of the GDPR are upheld.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person

Elena Kouremenou | Data Protection Officer
P +49 30 27576-425 | e.kouremenou@bitkom.org

Julia Tas | Legal Counsel
P +49 30 27576-335 | j.tas@bitkom.org

Responsible Bitkom committee

WG Data Protection
WG on Competition and Consumer Law