CIPL Response to the European Commission and the European Data Protection Board Public Consultation on the Draft Joint Guidelines on the Interplay between the GDPR and the DMA

Centre for Information Policy Leadership (CIPL)

4 December 2025

CIPL Response to the European Commission and the European Data Protection Board Public Consultation on the Draft Joint Guidelines on the Interplay between the GDPR and the DMA

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the joint draft Guidelines of the European Commission and the European Data Protection Board (EDPB) on the Interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR).

CIPL appreciates the cooperative nature of these draft Guidelines and the collaboration of the European Commission and the EDPB in providing guidance on the areas of overlap and tension between the DMA and the GDPR. While the DMA applies "without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation", we support the EC and the EDPB in their objective to provide guidance for coherent and consistent interpretation on the interplay between both laws, where personal data is involved. This is crucial to ensure legal certainty for organisations and clear, harmonised protection for users' rights across the EU digital landscape.

CIPL notes, however, that in several key areas, the draft Guidelines introduce interpretations that go beyond the DMA's legal text, potentially undermine GDPR protections, or create practical implementation challenges, while guidance is missing in some areas.

CIPL offers the following detailed observations and recommendations.

I. GENERAL OBSERVATIONS

1. The Guidelines should not create a primacy of DMA obligations

CIPL supports the premise of the draft Guidelines that the DMA and GDPR should be interpreted in a "compatible manner."[2] Specifically, the Guidelines should clearly acknowledge the distinct purposes, scopes, and legal bases of the two legal instruments and avoid conflating autonomous terms, definitions, and concepts in each law.

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] Draft Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation (the draft Guidelines), para 6.

The DMA's legal basis suggests it is not *lex specialis* to the GDPR,[3] and both instruments apply "without prejudice" to each other. CJEU case law confirms that when two EU acts of equal hierarchical value do not establish priority, they must be applied compatibly to ensure coherent interpretation.[4]

The GDPR is a fundamental rights instrument governing all processing of personal data that falls within its scope. It protects fundamental rights to privacy and data protection enshrined in the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union, while also ensuring the free flow of data. The DMA, by contrast, does not regulate or safeguard Charter-based rights, but is a competition and market-regulation instrument focused on contestability and fairness. Given these differing objectives, any guidance on their interplay must ensure that the DMA is interpreted and implemented in full respect of the GDPR's foundational role in protecting fundamental rights. The interpretation of DMA obligations must not result in lowering the level of data protection or privacy afforded by the GDPR, for the sake of the objectives pursued by the DMA.

2. Cooperation and enforcement between the DMA and the GDPR competent authorities should be clarified and more formalised in a legally binding act

Under the DMA, enforcement is entrusted to the European Commission, while the GDPR is interpreted, implemented, and enforced by national Data Protection Authorities and the EDPB. Recital 37 of the DMA makes clear that the Regulation applies "without prejudice" to the GDPR and its enforcement framework. Moreover, all authorities are bound by the principle of sincere cooperation, as reaffirmed by the CJEU in the *Bundeskartellamt* decision.[5]

While the draft Guidelines recognise the importance of cooperation between the Commission and EDPB/DPAs, they stop short of providing any more concrete proposals for an operational structure that could effectively support such cooperation. The current description of the "consultation" process is high-level and leaves important procedural aspects unspecified. Without a more robust framework, the risk of inconsistent interpretation of obligations and contradictory enforcement positions persists.

Given the non-binding nature of the Guidelines, such a cooperation framework may ultimately be most effectively created through a Union-level act that provides legal certainty, predictability, and accountability for all authorities and regulated entities.[6]

[3] See CIPL, *Limiting Legal Basis Under the DMA* (May 2023), p. 5-8. As the CIPL analysis explains, the Digital Markets Act is based solely on Article 114 TFEU, whose objective is the functioning of the internal market, and not on Article 16 TFEU, the specific legal basis for data protection. Because the DMA lacks this dual legal basis, unlike the AI Act, it cannot be regarded as regulating personal data processing as *lex specialis*, and therefore applies in parallel to, and "without prejudice" to, the GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf.

[4] Malta v Commission, T-653/16, paragraph 137.

[5] CJEU, Meta Platforms Inc and Others v Bundeskartellamt, C-252/21.

[6] See, for example, ideas proposed by the European Data Protection Supervisor (EDPS) in the Digital Clearing House 2.0, available at https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-01-15-towards-digital-clearinghouse-20_en.

II. SPECIFIC OBSERVATIONS

1. Article 5(2) DMA

a) The Draft Guidelines Rely on Undefined Terms that are Central to DMA Compliance

The DMA prohibits the combination and cross-use of personal data across core platform services, other gatekeepers, and third-party services. The DMA does not itself include any definitions, technical criteria, or boundaries. The draft Guidelines equally refer to "data combination" or "cross-use" but do not provide any further clarifications, despite these terms being central to Article 5(2) DMA.[7]

This creates significant legal and operational uncertainty. Gatekeepers cannot reliably determine which processing operations qualify as data combination or cross-use, which purposes fall within the DMA's scope, when consent is required, or when another legal basis could be appropriate.

Without clear definitions, organisations face the risk of both over-compliance (for example, unnecessary or overwhelming consent requests) and under-compliance (for example, inadvertent violations due to misinterpretation), to the detriment of users, innovation, and regulatory objectives. Any definition under the DMA must be tied to the Regulation's legal basis and scope, of "removing obstacles from the internal market", and should *not* inadvertently capture processing that is otherwise permissible under the GDPR (e.g., processing for security, fraud prevention, or service integrity).

Data combination or cross-use can cover a wide variety of processing operations, many of which do not relate to the DMA's core objective of increasing contestability.[8] In this regard, CIPL welcomes the acknowledgement in the draft Guidelines that processing can fall outside the DMA scope and will be subject to the GDPR in that case. This aligns with CIPL's interpretation that the DMA only applies to processing connected to its internal-market objective, and that all other processing remains governed by the GDPR.[9]

b) Providing separate interpretations under the DMA and the GDPR in the same guidance leads to confusion and legal uncertainty

The draft Guidelines, in paragraphs 67 to 77, address the cross-use of personal data between gatekeeper services that are provided together with or in support of each other, where user consent is not required. However, the draft Guidelines present two separate perspectives, one DMA and one

[7] May 2023, CIPL White Paper - *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences*, p. 13. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf.

[8] See CIPL, *Limiting Legal Basis Under the DMA* (May 2023), p. 14 and 17–18. The paper explains that "data combination" and "cross-use" may encompass a broad range of processing operations, many of which fall outside the DMA's contestability objective. Examples include cross-service signals used to detect child-safety risks (e.g., identifying suspected predators across services), detect age misrepresentation, identify coordinated ad-fraud behaviour, and correlate account-security incidents across products. These use cases illustrate that combination and cross-use often serve security, integrity, and safety purposes rather than competition-related objectives.

[9] CIPL White Paper - *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences,* p. 11.

GDPR, without any concluding observations or meaningful proposals for reconciling both. This creates confusion, particularly with respect to processing activities falling outside the scope of the DMA, where Article 6(1) (f) can provide an appropriate legal basis for cross-use and data processing.

c) Cybersecurity or fraud prevention, which often relies on data combination, can be based on Article 6(1)(f) GDPR

CIPL would like to point out that data combination and cross-use of data across platform ecosystems constitute one of the most effective tools for data security measures, allowing for the identification, detection, and prevention of sophisticated criminal activities.[10] We welcome that in the context of Article 5(2) DMA, the draft Guidelines reaffirm that data combination and cross-use for purposes such as network security, service integrity, fraud prevention, and ensuring user safety may be lawfully grounded in Articles 6(1)(c), (d), and (e) GDPR.

However, the practical application of these legal bases in this context remains significantly limited. Both Article 6(1)(c) ("necessary for compliance with a legal obligation") and Article 6(1)(e) ("necessary for the performance of a task carried out in the public interest") require that the underlying obligation or public-interest mandate be clearly established in Union or Member State law. Although certain EU and national instruments require organisations to implement cybersecurity or risk-mitigation measures, such as NIS2, DORA, or, to some extent, the GDPR itself, these provisions generally do not provide the level of clarity and specificity required to constitute a "legal obligation" under Article 6(1)(c) GDPR.

The scope of Article 6(1)(d) ("vital interest") is limited to cases of concrete and imminent danger to the data subject or third persons, and any preventative data security measures would often not qualify.[11]

Instead, data combination and cross-use for data security and fraud prevention might often be covered by the "legitimate interest" under Article 6(1)(f) GDPR. Recital 47 of the GDPR states expressly that "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned".

CIPL welcomes the draft Guidelines, acknowledging that gatekeepers may be able to rely on Article 6(1)(f) for data combination and cross-use of data if all cumulative conditions are met[12] and all other conditions of the GDPR are fulfilled[13]. However, the examples provided in the draft Guidelines are not sufficiently clear and do not, for example, include fraud prevention or cybersecurity.

In the context of Article 5(2) DMA and GDPR interplay, CIPL recommends that the Guidelines adopt clear definitions aligned with the scope of the DMA, provide sufficient and clear examples of

[10] CIPL White Paper - *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences.*
[11] See in more detail CIPL White Paper - *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences*, p. 18. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf.
[12] Draft Guidelines, paragraph 75.
[13] Draft Guidelines, paragraph 82.

processing activities that either do not require consent under Article 5(2) DMA or fall out of scope of the DMA entirely, and avoid splitting the guidance into a DMA and a GDPR view.

CIPL would also want to reiterate that the GDPR establishes no hierarchy among lawful bases under Article 6. All lawful bases are equally valid and equally protective when applied in accordance with the obligations of the GDPR. For this reason, the draft Guidelines' assumption that the DMA limiting gatekeepers' ability to select a legal basis under Article 6 GDPR and imposing consent "ensures a high level of protection of personal data" is not consistent with the GDPR framework. The level of protection does not stem from privileging consent over other lawful bases, but from ensuring that whichever basis is selected meets all of the GDPR's requirements. The guidance should therefore not be drafted in a manner that could be understood to suggest reduced protection when other lawful bases are appropriately applied.

d) Avoiding consent proliferation and choice fatigue

The DMA requires a single-purpose opt-in consent for cross-use and data combination. In a departure from the clear wording of the DMA, the draft Guidelines appear to effectively introduce a highly granular per-purpose opt-in model instead, in addition to the specific consent mechanisms already required under the GDPR for personal data processing. This represents a change in a regulatory approach that is not supported by Article 5(2) DMA. Interpreted strictly, this not only degrades the quality of the user experience but also diminishes the user's ability to comprehend the proposed choices meaningfully, leading to further choice and consent fatigue.[14] It would create practical challenges that the EDPB has previously recognised in the GDPR context: excessive fragmentation of consent flows reduces clarity, undermines informed decision-making, and generates administrative burdens without demonstrable privacy gains.[15]

In addition, the recently published Digital Omnibus amendments to the GDPR introduce new mandatory third-party consent requirements (new Article 88b GDPR). Under Article 88b, controllers must honour individuals' choices expressed via automated and machine-readable signals, including browser or device-level settings. Where users rely on such third-party mechanisms, it is uncertain how designated organisations under the DMA should operationalise Article 5(2) DMA-specific consent obligations concurrently.

Finally, the draft Guidelines include opt-in consent requirements for service development purposes, which would typically be considered under Article 6(1)(f) of the GDPR.[16] Imposing opt-in consent here appears disproportionate to the legislative objective of Article 5(2), especially where organisations can rely on data minimisation techniques and PETs/PPTs to limit or avoid the use of personal data.

[14] CIPL illustrates the scale of consent fatigue that would result from highly granular DMA-specific opt-ins layered on top of existing GDPR consent requirements. With just three GDPR consent choices (each accepted or declined), a user already faces eight possible configuration outcomes. When five additional DMA consents for cross-service processing are added, the number of possible configurations increases exponentially to 256, demonstrating how unworkable such an approach would be in practice, see CIPL Paper *Data Sharing Obligations under the DMA: Challenges and Opportunities*, p. 21-22, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_sharing_obligations_under_the_dma_-_challenges_and_opportunities_-_may24.pdf.

[15] EDPB Guidelines 05/2020 on consent under Regulation 2016/679.

[16] Draft Guidelines, paragraph 31.

The GDPR seeks to promote meaningful transparency and genuine user understanding rather than formalistic, repetitive consent interactions that are overwhelming and lead to "consent fatigue". In line with this objective, the final Guidelines should make clear that consent interfaces under the DMA may be delivered through contextual, layered flows, presented at appropriate, context-specific moments, and designed to minimise unnecessary friction. The Guidelines should further encourage dynamic, user-centric transparency approaches that align with the spirit of Recitals 32 and 42 of the GDPR, ensuring that individuals are empowered rather than burdened by the consent experience.[17] Depending on the service, this could be achieved, for example, by drawing on established DPA guidance for a layered approach with global control (e.g., 'Accept/Refuse All') at a first layer and the option to customize more granular, purpose-specific consents in a second layer.

e) Less personalised but equivalent alternative

The draft Guidelines note that: *the alternative service should not differ, in terms of performance, experience, and conditions of access* and then further specify that: "when the service for consenting users is offered by a gatekeeper free of monetary charge, the alternative service offered to non-consenting end users should also then, in principle, be provided free of monetary charge." The idea of a business within the EU providing a free service is not supported by the DMA provisions and goes against CJEU case law.[18] We would also caution that this is the subject of ongoing legal proceedings before the EU Courts. Embedding such language in the Guidelines at this stage may prejudge contested legal questions and create unnecessary uncertainty.

In this context, we would also like to point out that the introduction of a new "detriment" standard to assess the validity of consent without further analysis is problematic in light of the *Bundeskartellamt* decision, which suggests that subscription models can qualify as valid consent under the GDPR and DMA if they meet the required criteria.[19]

2. Article 6(7) DMA

CIPL would like to highlight that the draft Guidelines do not provide any information on the interplay between the DMA and the GDPR in the context of Article 6(7) of the DMA. Requiring gatekeepers to provide developers and businesses with free and effective interoperability with hardware and software features without ensuring equivalent safeguards, such as malware scanning, robust encryption, access-control integrity, and performance protections, can heighten system-level security risks and could expose both users and third parties to a number of risks, such as data breaches, device

[17] See CIPL Paper – *Design for Privacy: How Will the ePrivacy Regulation Affect Digital Services?*, p. 5–6 (emphasising that consent should be "timely" and presented at appropriate moments in context), p. 9–10 (highlighting that repetitive or front-loaded consent notices overwhelm users and fail to support meaningful engagement), and p. 17–18 (showing how contextual, layered and conversational privacy notices enhance comprehension and reduce friction). The study highlights that privacy controls should be embedded "throughout the UX, not just during first use," promoting dynamic, user-centric transparency that empowers rather than burdens individuals, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_design-for-privacy_may-2018_2_.pdf.

[18] CJEU, Meta Platforms Inc and Others v Bundeskartellamt, C-252/21.

[19] Leticia López Lapuente & Patricia Vidal, *Subscription models for digital services in the EU – Lights and shadows,* available at https://eulawlive.com/op-ed-subscription-models-for-digital-services-in-the-eu-lights-and-shadows-by-leticia-lopez-lapuente-and-patricia-vidal/.

compromise, and unlawful processing. Clear guidance is therefore essential to reconcile Article 6(7) interoperability with the GDPR's security and accountability requirements.

3. Article 6(9) DMA

We welcome several important clarifications in the draft Guidelines regarding the interpretation of Art. 6(9) of the DMA. In particular, paragraph 105 confirms that, as Article 6(9) DMA imposes a legal obligation on gatekeepers to enable data portability, the appropriate GDPR lawful basis for porting personal data under this provision is Article 6(1)(c) GDPR. This aligns with CIPL's analysis and provides much-needed legal certainty for organisations implementing DMA portability.[20] We also welcome paragraph 107, which clearly confirms that the scope of portable data expressly excludes derived or inferred data, ensuring consistency with both the GDPR and the approach taken in the Data Act.

However, the draft Guidelines fall short of addressing instances in which Article 6(9) goes beyond Article 20 of the GDPR in both scope and operational impact. Several aspects require further refinement to ensure legal clarity, technical feasibility, and alignment with the GDPR.

a) Operationalising "continuous and real-time" access

While Article 6(9) DMA refers to the "provision of continuous and real-time access," the Guidelines should introduce nuance regarding the practical implementation of this requirement. As drafted, the Guidelines risk creating expectations that many organisations subject to the DMA cannot technically or operationally meet. In practice, not all data is generated or processed in real time; existing systems are not uniformly architected for near-instantaneous extraction or synchronisation; and repeated or continuous data exports may jeopardise system performance, stability, and security. Accordingly, "continuous and real-time" should be interpreted as ensuring reliable access when needed, rather than obliging gatekeepers to maintain indefinite, uninterrupted data channels that may degrade system resilience or expose systems to exploitation.

A proportional, risk-based interpretation of this provision would better reflect technical and operational realities. Such an approach should take into account system design constraints, data-type characteristics, and security considerations, and would recognise that periodic or event-based updates, such as daily refresh cycles, may offer the most appropriate balance between user benefit and operational viability. This should include recognition that users should have granular control over the duration of access, such as one-time access, access for a fixed period, or ongoing access until withdrawn, supported by clear renewal mechanisms. Gatekeepers should similarly be permitted to introduce reasonable maximum access periods (for example, yearly increments) to mitigate security risks, including fraud, credential stuffing, account takeover, and misuse of stale tokens. These controls would ensure that access remains user-directed, time-bounded, and aligned with best-practice security protocols.

This will require further clarification regarding the boundaries of "generated data." For example, data residing solely in disaster recovery systems or similar inactive sources that would require disproportionate technical effort to restore, should be excluded.

[20] CIPL Paper Data Sharing Obligations under the DMA: Challenges and Opportunities, p. 7.

In the same manner, on-device data is frequently protected by hardware-based encryption specifically to prevent extraction. Mandating its export could require circumventing these local security enclaves, creating new attack surfaces.

It is therefore essential that the final Guidelines adopt a nuanced interpretation consistent with the principle that obligations introduced under the DMA must remain firmly anchored in its internal-market legal basis. They cannot mandate technically unworkable or disproportionate interventions that introduce disproportionate risk to the end user or the service and exceed what is necessary to address the specific competitive concerns the Regulation seeks to remedy.

b) Safeguards for Third-Party Data and Authorised Recipients

The Guidelines should provide clearer direction on the treatment of personal data relating to third parties. Article 20 GDPR already contains a well-developed framework for handling such data in portability requests, including safeguards to protect the rights and freedoms of other individuals. This requires third-party data to be redacted, pseudonymised, or otherwise protected, and that only data directly provided by or observed from the requesting user should be included unless appropriate safeguards exist. DMA portability obligations must not undermine the GDPR's core principles or generate new risks for data subjects.

In this respect, the interpretation set out in paragraphs 105–106 of the draft Guidelines, namely, that DMA Article 6(9) portability operates independently of GDPR compliance and relieves gatekeepers of responsibility for ensuring third-party data protection, should be reconsidered. It conflicts directly with how similar data-sharing and portability rights are structured under the Data Act, which explicitly preserves the primacy of the GDPR. Article 1(5) of the Data Act confirms unequivocally that any processing of personal data carried out pursuant to its data-sharing obligations must remain fully subject to the GDPR.

This gap in the interpretation of Article 6(9) is particularly striking when contrasted with the very high level of protection the draft Guidelines affords to search-data disclosures under Article 6(11) DMA. Article 6(11) requires *any* personal data contained in the shared data to be anonymised. This would presumably extend to third-party data. Yet no comparable safeguards are applied to Article 6(9), even though portability may involve the disclosure of far more sensitive or intrusive categories of personal data.

This asymmetry creates a significant inconsistency: the Guidelines permit the transfer of fully identifiable personal data, of third parties, to authorised recipients under Article 6(9) DMA, while Article 6(11) GDPR, and the Data Act set a different standard. Such a disparity risks undermining both the GDPR's protective framework and the DMA's objective of fostering safe, trusted, and contestable markets. Designated companies should be permitted, and, where risks warrant, required, to conduct proportionate pre-transfer safety and security vetting of third-party data recipients to prevent misuse, exfiltration, or similar misuse of personal data. This could include verifying requester authenticity, assessing indicators of fraud or malicious intent, and ensuring that the recipient has an adequate security posture. End-users must have the opportunity to be informed and find protection from nefarious actors, data-harvesting operations, and other security threats.

c) International data transfers

The draft Guidelines (paragraphs 132–136) address international data transfers in the context of Article 6(9) of the DMA, including how these transfers should be treated under the GDPR. In this regard, it is important to note that the DMA data portability provisions do not override GDPR rules on international data transfers. Any transfer of personal data outside the EEA that arises as a consequence of user-initiated portability must continue to comply fully with Chapter V GDPR.

The draft Guidelines suggest, inter alia, that transfers carried out pursuant to user-initiated portability may rely on the derogations in Article 49(1) of the GDPR.

This is inconsistent with EDPB guidance, which provides that Article 49 derogations are exceptional in nature and cannot be relied upon for repetitive, structural, or continuous transfers.[21] DMA portability mechanisms, particularly where framed as continuous or real-time access, would, however, likely have to be considered as falling within the category of repetitive and systematic transfers, thus excluding Article 49 derogations in accordance with EDPB guidance.

Any implication that DMA obligations could legitimise such reliance risks creating significant legal uncertainty for gatekeepers and data controllers at large. The DMA cannot be interpreted as permitting or compelling transfers that lack an appropriate transfer mechanism, nor as diminishing the requirement for transfer impact assessments and appropriate safeguards. The Guidelines should make this explicit or clarify whether Article 49 derogations can be applied to more frequent data transfers in general.

The Guidelines must clarify that DMA portability obligations do not modify, relax, or supersede Chapter V of the GDPR, and that all international transfers carried out under Article 6(9) must be fully compliant with the GDPR's transfer mechanisms and risk-assessment requirements.

4. Article 6(10) DMA

a) Scope of business-user access and allocation of controller responsibilities

Article 6(10) has been the subject of considerable uncertainty, and some aspects of the draft Guidelines appear to expand the provision beyond the DMA's text. This risks creating obligations that neither the Regulation nor its legal basis supports.

The DMA clearly restricts the access right to personal data that is generated "in respect of the products or services of the business user" as offered through the gatekeeper's core platform service. However, the draft Guidelines repeatedly frame the scope more broadly as relating to "end-user activity within the CPS," which would, as a result, include data concerning the gatekeeper's own services, interactions unrelated to the business user, or data about third parties with whom the business user has no relationship. This interpretation is inconsistent with the text and structure of the DMA and risks turning a targeted access right into a much broader disclosure obligation. The Guidelines should be aligned with the DMA's wording and legal intent, and the DMA obligations must remain limited to

[21] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 3-4.

processing linked to the Regulation's internal-market purpose and cannot be expanded to cover activities outside its scope.

The draft Guidelines also suggest that gatekeepers should ensure that business users obtain "valid" consent from end users before accessing personal data. This is not supported by the DMA. Business users act as independent controllers and bear full responsibility for securing GDPR-compliant consent where required. Gatekeepers may technically facilitate consent collection, but cannot be made accountable for verifying the lawfulness or validity of business-user consent. Such an approach would contradict the controller-responsibility framework of the GDPR and improperly shift accountability to gatekeepers. The draft Guidelines should therefore correct this implication and clearly reflect the responsibilities established by both the DMA and the GDPR.

b) Record-keeping obligations consistent with GDPR principles

Paragraph 154 of the draft Guidelines suggests that gatekeepers should "keep a record of all categories of data, including personal data," to demonstrate compliance with Article 6(10) DMA, and frames this as a separate obligation from Article 30 GDPR. This creates considerable uncertainty, as the draft Guidelines do not specify whether such record-keeping refers merely to a high-level overview of available data categories or to an obligation to retain the underlying data itself.

A broad understanding of the record-keeping obligation would be in direct conflict with the GDPR's data-minimisation principle, storage-limitation principle, and best practices for data hygiene, which encourage organisations to avoid unnecessary data retention. It would also contradict the longstanding approach under Article 30 GDPR, which requires controllers to document processing activities, not to retain or catalogue all data that may be processed or accessible in a system. Importantly, there is no such record-keeping obligation under the DMA itself: Article 6(10) requires gatekeepers to ensure and be able to demonstrate "effective compliance," but it does not prescribe, nor imply, a duty to maintain comprehensive catalogues of all data categories. Demonstrating effective compliance can be achieved through a range of appropriate organisational and technical measures, such as governance documentation, systems-level design explanations, or audits, without imposing a de facto data-retention or data-inventory mandate.

The Guidelines should therefore be revised to clarify that Article 6(10) does not impose a new data-retention obligation and that any record keeping must remain fully consistent with GDPR requirements.

5. Article 6(11) DMA

a) Risk-based anonymisation standard

Article 6(11) obliges gatekeepers to protect against re-identification of personal data shared as part of a query, click, or view data by, for example, anonymisation, but without degrading data utility for the data recipient. CIPL welcomes, in this context, that the draft Guidelines refer to the qualification of Recital 26 GDPR, which recognises that anonymisation is inherently risk-based and must be assessed by reference to "all the means reasonably likely to be used" for re-identification, rather than hypothetical, unlimited or adversarial capabilities.

However, as currently framed, the standard, articulated in the draft Guidelines, would, in practice, require an *effective anonymisation*[22] outcome that leaves no realistic possibility of residual identifiability, while simultaneously acknowledging the inherent richness of search data[23].

An assessment of the means and potential intent especially of hypothetical, unknown third parties, to re-identify individual end users is ill-suited to the context of controlled B2B transmissions under Article 6(11). The draft Guidelines establish a threshold that is operationally unachievable and, given that the GDPR mandates a risk-based approach to processing, it places gatekeepers in a position of regulatory conflict: personal data cannot be anonymised to the required standard, while the DMA compels its sharing.

The final Guidelines should therefore adopt a GDPR-consistent, risk-based standard for anonymisation, focused on eliminating the reasonable likelihood of identification rather than requiring unattainable guarantees. They should embrace a pragmatic solution that leverages contractual controls, for example. As acknowledged in the context of potential future Implementing Acts, such legally binding restrictions on onward transfer can mitigate residual risks. Recognizing these safeguards now would allow the technical risk assessment to be properly calibrated to the *intended* recipient, ensuring the data remains actionable for contestability purposes without compromising privacy. The Guidelines should also explicitly encourage the use of privacy-enhancing technologies, such as differential privacy, synthetic data generation, secure multiparty computation, and homomorphic encryption, which can materially reduce re-identification risk while enabling meaningful access to data. This is essential for making Article 6 (11) DMA workable in practice.

The position articulated in the draft Guidelines in relation to Art. 6 (11) DMA must also be aligned with forthcoming EDPB guidance, which is expected to revise existing anonymisation and re-identification risk assessments in light of the *SRB* judgment and the proposed Digital Omnibus amendments. Any fixed or absolute anonymisation standard may be out of step with the evolving and more harmonised EU-level interpretation of anonymisation under the GDPR.

Key Recommendations

In the context of the draft Joint Guidelines of the European Commission and the European Data Protection Board (EDPB) on the interplay between the DMA and the GDPR, CIPL recommends that the final Guidelines:

- Clearly confirm that the DMA is not lex specialis to the GDPR and that both instruments must be interpreted compatibly, in full respect of the GDPR's fundamental-rights framework.
- Avoid expanding DMA obligations beyond the legal text by introducing interpretations that undermine GDPR protections or impose new compliance burdens without a legislative basis.
- Provide clear definitions of "data combination" and "cross-use" under Article 5(2) DMA, aligned with the Regulation's internal-market objective.

[22] Draft Guidelines, para 186.
[23] Draft Guidelines, para 185.

- Confirm that processing falling outside the DMA remains fully governed by the GDPR, including lawful reliance on Article 6(1)(f) for security and fraud-prevention purposes.
- Avoid consent proliferation by supporting layered, contextual, and user-centric consent mechanisms and rejecting unnecessary per-purpose opt-in models.
- Remove any suggestion that alternative services must be provided free of charge and avoid prejudging ongoing legal proceedings.
- Clarify that DMA consent obligations must not displace the GDPR's lawful-basis framework or create a hierarchy among legal bases.
- Introduce operational guidance on cybersecurity safeguards in relation to interoperability obligations under Article 6(7) DMA.
- Interpret "continuous and real-time" access under Article 6(9) proportionately, allowing for technically feasible and risk-based implementation models.
- Ensure that portability under Article 6(9) fully respects GDPR safeguards for third-party personal data.
- Explicitly confirm that DMA portability does not override GDPR Chapter V and that international data transfers must remain fully compliant with GDPR transfer rules.
- Limit Article 6(10) access rights to data generated in relation to the business user's own services and reaffirm that business users bear sole responsibility as controllers.
- Clarify that Article 6(10) does not create new data-retention or inventory obligations beyond Article 30 GDPR.
- Adopt a GDPR-consistent, risk-based standard for anonymisation under Article 6(11), supported by contractual and technical safeguards.
- Encourage the use of privacy-enhancing technologies such as differential privacy, synthetic data, and secure computation to reduce re-identification risk.
- Establish a formal and legally binding co-operation framework between the European Commission and other relevant authorities to ensure coherent enforcement.