CONTRIBUTION TO THE PUBLIC CONSULTATION ON THE JOINT COMMISSION–EDPB GUIDELINES ON THE INTERPLAY BETWEEN DMA AND GDPR

Foreword

Data Rights warmly welcomes the opportunity to respond to this consultation on the Joint Draft Guidelines on the Interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR) by the European Commission (EC) and the European Data Protection Board (EDPB).

Data Rights works to build an internet free from monopolistic control and surveillance is a business model. An internet where NGOs, businesses, and individuals are not left technically exposed, and where exercising basic rights does not depend on the goodwill of a few tech giants. Everyone, citizens, communities, organisations, and critical infrastructures, must have access to cybersecurity and human rights safeguards that allow them to thrive with dignity and autonomy.

Data Rights believes interoperability and data portability enforcement to be the key. We seek to foster the diversification of digital ecosystems, to the benefit of individuals and society. We see the EU's the Digital Markets Act (DMA) as a timely opportunity to leverage data mobility obligations to create change. By using the expertise of competing businesses and guiding users, we can bring together actors to challenge structural power imbalances and enable digital self-determination. Moving between services and exchanging across platforms in real time should be an act of digital self-determination. Shifting data shifts power.

The DMA aims to become a pillar of user empowerment and market contestability in the European digital society. Its interaction with the General Data Protection Regulation (GDPR) is tangible, be it via formal signposting in its clauses as well as through the fact that competition authorities have been grappling with the need for them to join forces with their data protection counterparts to tackle causes of harm online rather than symptoms.

Looking at the GDPR, a recital must be pointed out: “[…] consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller […]” (Recital 43, GDPR). This law enshrines that power imbalances prohibit a stronger party from requesting the weaker party to consent for the processing of their personal data. This for instance translates into one’s manager or employer being prohibited from asking for their consent to take pictures of them and put them on the company’s website, unless it is a necessity for the employment contract.

The DMA is therefore conditioning most of its processing of personal data to a legal basis that was created to not apply to situations of power asymmetry. That is, the situations it regulates. Situations where a party, the gatekeeper, is so powerful that users might not feel they can afford to refuse anything to. That is, if they even get to the position where they feel they understand exactly the practical implications if they say yes, and if they say no.

In addition, gatekeepers are entities that yield so much power that their resources enable them to influence regulators, slow their work in any ways possible and sometimes dodge compliance altogether.

Consent must not mean capitulation

Aside from data protection law practitioners, a frequent misconception about the notion of consent is that it empowers. Yet as stated above, it only does empower in contexts where one choses to consent, free of power dynamics. It will be a real tour de force to construct a rights affirming environment in relationships between users and the most powerful companies, companies often behaving or treated as public digital infrastructure. Companies without which it is virtually impossible for anyone not tech savvy to stay in touch with their family or have strong job opportunities.

The example of cookies regulation via the ePrivacy Directive might helpfully teach lessons. The ePrivacy, like the DMA, aims at regulating technical features of our increasingly digitalising societies. The root of the ePrivacy’s consent requirement was the idea that cookies present such a high cybersecurity risk for individuals, via the injection of executable code on individual’s devices, that it needed to be conditioned to the most empowering legal basis. This resulted in powerful lobbies working hard to create confusion around how cookies were to be regulated, ultimately managing to turn consent into a transactional commodity. If one wishes

to access interesting content they will need to give away their data to an unclear number of companies, and their partners, and these partners' partners. This tremendous effort enabled powerful players to have small businesses and users develop frustration at the notion of consent. Small businesses pay for banners they do not understand and, usually, breach the law, while users feel harassed in the name of their rights. Nefarious compliance has become the norm, not the exception.

Consent cannot lead to shifting the onus on users, for having somewhat 'freely' chosen to tie themselves to a dubious company. In other words consent is a double edged sword, if it is not empowering, it is disempowering in egregious ways.

The GDPR does add a nuance that did not exist at the time of ePrivacy: the accountability principle. This fundamental principle participates to making the GDPR future-proof, by infusing compliance with the idea that what will be expected from an entity in terms of compliance will be influenced by a company's size, type of data processed, or context. In other words, the accountability principle implies that a greater compliance burden is born by the most powerful players. More specifically, the GDPR leaves multiple notions to be defined by what is best practice at the time of processing, for instance the concept of compliance by design and by default. Applying the accountability principle could imply that the most powerful players' data processing activities must reflect nothing less than exemplar best practice where it comes to consent management.

***

The submission bellow is solely done in the name of Data Rights, although it does reflect some of the preparatory work involving friend organisations that responded to this consultation too. We greatly appreciated their kind support, while our capacity is still being built.

We welcome the Joint Draft Guidelines on the Interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR) by the European Commission (EC) and the European Data Protection Board (EDPB). The Draft Guidelines represent a constructive step toward consistent enforcement across regulatory frameworks. They correctly reaffirm that the DMA and the GDPR are complementary, not conflicting, regimes. Data Rights particularly welcomes the emphasis on valid consent; the reference to data protection by design and by default; the recognition that gatekeepers cannot rely on legitimate interest or contractual necessity for processing under Article 5(2) DMA; and the

explicit attention to deceptive design (so-called 'dark patterns'). The Guidelines are a welcomed joint effort between the EC and the EDPB that reaffirms that healthy competition is key to upholding fundamental rights, and therefore reinforcing one another.

That said, the Guidelines should also ensure that upholding the rights under the GDPR is paramount, and should not be subordinated to political or market considerations. Below are our main observations and recommendations.

1. Overall framing and hierarchy of norms

The Guidelines repeatedly describe the DMA and the GDPR as frameworks that should be 'interpreted and applied in a compatible manner.' We support this approach but stresses that compatibility does not mean equivalence. The GDPR has a constitutional foundation to uphold data protection rights which are also protected under the Charter of Fundamental Rights of the European Union (EU Charter). The DMA—although primarily an economic regulation intended to promote market contestability and fairness—is also intended to reinstate and protect the rights and interests of users, in particular having regard to their privacy and data protection. The Guidelines should therefore explicitly confirm that when tensions arise, upholding the user's right to privacy (Article 7 EU Charter) and data protection (Article 8 EU Charter) and the rights of data subjects under the GDPR must prevail. The current wording seems to imply that in case a conflict arose between fundamental rights on the one hand and market contestability and fairness goals on the other, the latter could prevail, which would contradict the principle of primacy of fundamental rights as enshrined in EU law. For example, paragraph 6 stresses that the two frameworks should be applied in a way that 'maximises achievement of the respective objectives' of both the DMA and the GDPR. This wording could be interpreted as allowing concessions for market-related goals, unless the primacy of upholding fundamental rights is explicitly reaffirmed.

We therefore recommend:

- Inserting an explicit reference to Article 52(1) of the Charter to clarify that any limitation on rights in the Charter must respect the essence of those rights and meet the test of necessity and proportionality;
- Clarifying that attempting to comply with obligations under the DMA does not in itself create a lawful basis for processing under GDPR. Any processing carried out in the context of complying with the DMA must still rely on an existing legal basis under Article 6 GDPR and meet all corresponding principles, including purpose limitation, necessity, and data minimisation;
- Ensuring that the 'coherent application' goal must not lead to mutual dilution of enforcement.

2. Article 5(2) DMA and consent under the GDPR

The section on Article 5(2) DMA is the strongest part of the Guidelines, but several points could benefit from improvements to avoid interpretative ambiguity.

a. Consent and the risk of manipulation by gatekeepers

The Guidelines confirm that gatekeepers cannot rely on legitimate interest or contractual necessity for processing covered by Article 5(2) DMA. While it is very welcome that the Guidelines reconfirm the EDPB's position that 'Consent or Pay' models are incompatible with Article 5(2) DMA and with the GDPR requirements for freely given consent, the text should also more clearly reiterate that consent cannot not be valid when data subjects have no real choice due to the gatekeeper's overwhelming market power.

Moreover, the Guidelines stop short of explicitly prohibiting coercive practices in the DMA context. A gatekeeper that forces users to accept processing or to pay in order to access equivalent services is not obtaining valid consent under the GDPR. The Guidelines should explicitly refer to Recital 36 DMA to reaffirm that users must not be forced to choose between paying with money or paying with data.

We recommend clarifying that:

- Any 'less personalised but equivalent' service must always—not only in principle—be offered without monetary charge when the main service is free of charge, in line with the Commission's decision in Meta (Article 5(2));
- The notion of equivalence includes equal accessibility and functionality, not only interface parity;
- Practices that monetise a data subject's refusal to allow the processing of their personal data violate both Article 5(2) DMA and Articles 4(11) and 7 GDPR.

b. Deceptive consent design

The Guidelines correctly refer to the need to ensure compatibility between Article 5(2) DMA, the GDPR and other consumer-law standards when gatekeepers choose their user interface design. However, the examples provided remain abstract. Gatekeepers are already deploying deceptive design tactics that exploit users' cognitive bias by encouraging a user to opt for a particular consent option based on the design. For example by choosing bold type faces or eye-catching colours, these tactics are increasingly being used by gatekeepers as a lucrative loophole to claim compliance. The Guidelines should set out concrete operational criteria and explicitly link design obligations to related frameworks, such as the Digital Services Act and the ePrivacy Directive (more on this below). This cross-reference would ensure consistency in the treatment of deceptive or manipulative interfaces across EU laws and prevent gatekeepers from exploiting gaps between instruments. Operational criteria on consent design could include for instance:

- An explicit prohibition of unequal visual design, such as colouring 'accept' buttons more prominently than 'reject;'
- A requirement for symmetry in timing and effort between granting and refusing consent, both at the initial choice and whenever the user wishes to change their decision;

- An obligation on gatekeepers to allow users to withdraw their consent as easily as it is for them to give consent, without additional steps or penalties.

In addition, the Guidelines should recall that Article 13(6) DMA and Article 25 GDPR jointly require privacy-preserving design choices, not only compliant wording. Requiring 'neutrality' in design should be linked to the principle of fairness and not presented as a mere usability matter.

c. Limitation on repeated consent requests

The one-year limitation on repeated consent requests is important but should be reinforced. The Guidelines should clarify that any modification of the interface or rewording that does not change the processing purpose counts as a repetition. The text should also specify that circumvention via A/B testing, personalised prompts, or changes in the order of choices would breach Article 13(4) DMA. It would be useful to link this explicitly to the EDPB's work on choice fatigue and to clarify enforcement responsibility between the Commission and supervisory authorities (SAs).

d. Processing without consent under Article 6(1)(c)–(e) GDPR

While the Guidelines rightly limit alternative legal bases to strict cases, they could better define their boundaries. The reference to 'security purposes' is too vague. Gatekeepers have historically stretched the notion of security to justify tracking and profiling. The Guidelines should specify that Article 6(1)(c) applies only where processing is required by law, not by internal policy, and that 'vital interests' and 'public interest' grounds are exceptional. Without such clarity, the clause risks being used to rebuild the legitimate-interest loophole that Article 5(2) intended to close.

3. Interoperability under Article 7 DMA

We welcome the Draft Guidelines' clear recognition that 'from a data protection point of view, implementing a well-defined protocol for managing the exchange and certification of cryptographic keys between gatekeepers and providers of NIICS requesting interoperability would greatly contribute to a secure foundation for a reliable implementation of E2EE.' While the DMA does not prescribe any specific messaging protocol or encryption method, it becomes evident that—for the purpose of securely implementing Article 7 DMA—the use of open, interoperable protocols is largely superior in the long run, as compared to the gatekeeper offering proprietary APIs.

In this context, we also welcome the Draft Guidelines' insistence on minimising the processing of metadata as well as the implementation of cryptographic authenticity verification methods in the context of messaging interoperability.

The interoperability provisions are very positive for user rights, yet raise data protection questions that are already well-known from other federated communications systems. The Guidelines mention the need for data minimisation and proportionality but remain vague on who bears responsibility as data processor in the context of interoperability. In order to prevent gatekeepers from relying on this to delay or refuse interoperability under the guise

of Article 7(9) DMA's integrity, security, and privacy exemptions, the Guidelines should re-affirm that each party remains responsible for the processing of personal data initiated on their side, in line with GDPR and existing case law. At the same time, the gatekeeper should continue to be allowed to raise genuine security risks where strictly necessary. In order to prevent gatekeepers from using this exception as a basis to delay or refuse interoperability, the Guidelines should give practical examples of such strict necessity that support the implementation of messaging interoperability without diminishing user rights or security.

4. Data access and portability (Articles 6(9)–6(11) DMA)

The Guidelines provide a useful interpretation of these rights. They should also ensure that portability and access do not lead to reduced user controls over the processing of personal data. In particular, the Guidelines should clarify that transfers of data to non-EU/EEA countries without adequacy should be subject to the same conditions as under Chapter V GDPR, including assessment of access by public authorities.

The anonymisation requirements under Article 6(11) DMA are described only briefly. Given the repeated failures of anonymisation by the industry in the past, the Guidelines should reference Recital 26 GDPR, the EDPB Guidelines 01/2025 on Pseudonymisation, and the Court of Justice's recent judgment in EDPS v SRB (C-413/23 P, 4 September 2025). In that case, the Court clarified that pseudonymised data may still constitute personal data when the controller retains, or has access to, information enabling re-identification, and that identifiability must be assessed contextually and from the controller's perspective at the moment of collection.

As the Court confirmed, pseudonymisation may, in some cases, lead to anonymisation only if effective technical and organisational measures truly prevent re-identification by any party reasonably likely to have access to the data. However, the judgment also underscored that such claims must be demonstrated, not presumed. The ruling should not be read as a relaxation of standards: anonymisation still requires a full risk assessment, a defined threat model, and proof that re-identification is not reasonably possible given situationally relevant attackers and contextual factors.

Accordingly, any anonymisation method used under Article 6(11) must be transparently documented, subject to independent technical verification, and compatible with the standards established by Recital 26 GDPR as well as the EDPB's pseudonymisation (and future anonymisation) guidance. They should also explicitly warn that controllers cannot rely on formalistic or recipient-based arguments to claim anonymisation without evidence of effective de-identification. The Guidelines should therefore emphasise transparency, disclosure of the methods used, and independent oversight.

This assessment cannot be delegated to contractual assurances or internal policies. The Guidelines should therefore require independent technical verification of any claimed anonymisation technique, supervised by the Commission in cooperation with supervisory authorities. Without external oversight, anonymisation risks becoming a discretionary

assessment by the gatekeeper rather than an objective legal threshold, which would undermine both fundamental rights and the effectiveness of Article 6(11) DMA.

5. Risks from parallel deregulatory initiatives (Digital Omnibus on Data)

The forthcoming Digital Omnibus on Data includes several proposals that illustrate the growing trend to diminish fundamental concepts of data protection in ways that prioritise market convenience over protecting rights. All of these changes have the potential to empower businesses and authorities while disempowering data subjects. In particular, several of its provisions will directly affect the compatibility of the DMA–GDPR relationship. Most notably, the proposal's suggestion to expand the use of legitimate interest as a legal basis for AI development and training would create an explicit contradiction with Article 5(2) DMA. Introducing legitimate interest as an alternative lawful basis for large-scale model training would effectively allow the same data aggregation that the DMA was designed to prevent, undermining both user autonomy and market fairness.

The Digital Omnibus also includes proposals for the adoption of delegated or implementing acts defining anonymisation and pseudonymisation standards. Such a power would permit the executive to determine, through secondary legislation, when data ceases to be personal. This approach conflicts with the Court's case law in Breyer (C-582/14) and EDPS v SRB (C-413/23 P), both of which affirm that defining personal data is an objective, technology-neutral legal test that cannot vary by controller or administrative act. Allowing the Commission to set these standards would blur the boundary between personal and non-personal data, and diminish its fundamental rights standard to an administrative category, weakening the application of the GDPR and fragmenting enforcement of the DMA.

We are also alarmed by the European Commission's announcement as part of the 'Digital Fitness check' that any of the EU's digital laws could be reopened in the next years. As the Commission's staff working document specifically mentions DSA and DMA, we are adamant that this will likely lead to rolling back crucial individual and market protections provided by those laws that currently make Europe a global leader.

We therefore recommend that the Guidelines explicitly exclude any incompatibility between the DMA's Article 5(2) consent requirement and any possible new legal bases that are being discussed that would allow gatekeepers to reuse data for AI training without freely given and explicit consent. They should also reaffirm that only the legislator and the Court of Justice, not the executive, may interpret the scope of personal data and anonymisation. Preserving the objective definition of personal data is essential to upholding the rights to privacy and data protection as outlined in the EU Charter. Such proposals seek to diminish data protection rights in favour of innovation. As well as the DMA's role in addressing the data exploitative practices common in digital markets today. They also create loopholes for industry to circumvent compliance.

6. Coordination and enforcement

The cooperation section recognises the need for alignment between the Commission and SAs but underplays structural asymmetry. Under the DMA, the Commission is the sole enforcer, while under the GDPR, enforcement is decentralised. Without clear procedural guarantees, there is a risk that the Commission's interpretation will effectively shape data protection enforcement. To prevent this the Guidelines should state:

- That the Commission's enforcement of the DMA should complement, not replace, the responsibilities of national SAs under the GDPR;
- Any exchange of information should comply with Article 62 GDPR and ensure protection of investigative confidentiality;
- When the Commission's findings indicate possible GDPR breaches, meaningful cooperation with the competent SA should be mandatory, not optional. Such cooperation procedures should not lead to a delay in DMA enforcement.

It would also be beneficial for the Guidelines to mention the need for joint case handling protocols, transparency on data exchanges between authorities, and public communication consistent with the GDPR's accountability principles.

7. Interaction with the ePrivacy Directive

The Guidelines mention the ePrivacy Directive (ePD) only in passing. Given that Article 5(3) ePD governs access to information in terminal equipment, including cookies and identifiers, the Guidelines should make clear that compliance with the ePD is a precondition for lawful processing under both the DMA and the GDPR. A gatekeeper cannot rely on Article 5(2) DMA consent to override the requirements of Article 5(3) ePD. The final text should explicitly acknowledge this hierarchy and avoid treating ePrivacy as merely optional.

8. Addressing collective and structural harms

The current framing of the Guidelines risks overlooking the structural and collective dimensions of data exploitation by gatekeepers. Article 5(2) DMA was introduced not only to safeguard individual consent but also to address systemic market imbalances arising from data concentration. Similarly, the GDPR embodies collective dimensions through its principles such as fairness, transparency, and accountability, which require controllers to consider broader societal risks. The Guidelines should integrate this perspective by:

- Referencing collective or societal risks in the interpretation of proportionality and fairness;
- Encouraging SAs and the European Commission to consider aggregated harms in enforcement cooperation;
- Recognising that data-driven advantages are not neutral market efficiencies but forms of structural inequality.

9. Conclusion

The joint Guidelines are a promising foundation for consistent enforcement of the DMA and the need to ensure the full application of the GDPR to the practices of gatekeepers.

They correctly frame compliance with both frameworks as mutually reinforcing rather than mutually exclusive. To fully achieve this goal however, the Guidelines must clarify the primacy of fundamental rights, limit the scope for gatekeeper manipulation of consent, reinforce data minimisation obligations, and ensure strong cooperation that does not undermine the autonomy of SAs.

A coherent digital regulatory framework will only exist if the DMA's competition objectives serve, rather than compromise, the protection of personal data and the autonomy and rights of individuals. The Guidelines should make this principle explicit.

***