

Comments of the International Center for Law & Economics

*RE: Joint EDPB-European Commission Guidelines on the
Interplay Between DMA and GDPR*

4 December 2025

Authored by:

Mikołaj Barczentewicz (Senior Scholar, International Center for Law & Economics)

Executive Summary

We thank the European Commission (the Commission) and the European Data Protection Board (EDPB) for launching this consultation on their draft joint guidelines (Draft Joint Guidelines) on the interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). ICLE is a nonprofit, nonpartisan research centre that applies law & economics methodologies to analyse technology governance, competition, and consumer-protection policy. Our interest is to ensure that the EU's digital rulebook advances consumer welfare and innovation through clear, predictable, and proportionate rules grounded in evidence and sound economics.

The approach adopted in the Draft Joint Guidelines will lead to a new proliferation of “consent popups” at a time when the Commission is seeking to address similar past failures of EU law regarding “cookie banners”. Users of digital services regulated under the DMA are likely to see further declines in the quality of their experience, and this could further damage the reputation of EU law. The DMA's goals do not necessitate this approach, and we encourage both the EDPB and the Commission's DMA Team to address the issue of consent in a more user-friendly way.

The guidelines disproportionately contradict the aims of EU data protection and cybersecurity laws by requiring that gatekeepers do not warn users about clear and realistic risks that attend data portability (especially real-time and continuous portability) and by preventing gatekeepers from excluding known bad actors as recipients of user data. Effectively, the Draft Joint Guidelines would even mandate that gatekeepers support and enable campaigns by criminal or foreign-enemy-state actors to collect EU personal data, so long as those actors inform the gatekeeper—even falsely—that they're EU organisations and don't plan to transfer personal data outside the European Economic Area (EEA).

More generally, the guidelines depart from previously stated Commission policy, supported directly by the DMA, that gatekeepers have a duty to ensure DMA-implementation measures comply with other laws, including those on data protection and cybersecurity. Instead, the Draft Joint Guidelines propose to prohibit gatekeepers from implementing the most effective measures to achieve such compliance.

The guidelines interpret the DMA and the GDPR inconsistently. Without appropriate justification, some serious data-protection risks (e.g., those related to data portability) are not addressed as robustly as others (e.g., the sharing of search data).

The Draft Joint Guidelines also omit interoperability mandates under Article 6(7) DMA, incorrectly suggesting that such obligations pose no serious privacy issues. In fact, such issues include questions regarding the interplay between the DMA and the GDPR, as well as the ePrivacy Directive.

I. Proliferation of Consent Requests (Articles 5(2), 6(10) DMA)

The European Commission last month proposed legislation to address the problem of “cookie consent fatigue” by changing rules that are “outdated and inadequate for contemporary privacy and data needs”.¹ It is therefore surprising to see the EDPB and the Commission’s DMA team pursue guidelines that would vastly increase the proliferation of consent requests with which EU users of digital services are bombarded.²

The excessive reliance on ever-more consent requests, without any investigation of ways to reduce the need for them in accordance with the law, flies in the face of the current research on data protection. Even vocal critics of the ways that digital services use personal data recognize that the consent-centric approach has been a failure.³

We should expect more from public authorities than the unthinking application of the consent paradigm, while failing to address the actual problems of data protection and security.

The Draft Joint Guidelines contribute to the disproportionate proliferation of consent requests in the following ways:

- Consent requests for the use of third-party data for online advertising, combining and cross-using personal data (Article 5(2) DMA) are meant to be further divided into various “purposes” like “personalisation of content, personalisation of advertisements, and service development”.⁴ While the guidelines direct gatekeepers to combine DMA and DMA-GDPR requests, avoiding the need to further double many consent requests, this doesn’t address the increased consent fatigue that users will experience.⁵
- The Draft Joint Guidelines’ section on “ensuring user-friendly choices and consent designs”⁶ is a stark example of what has been dubbed the “nerd harder” approach,⁷ without providing much actionable guidance on consent design. In its preoccupation to present choices in a “neutral” manner, the section fails to propose even the contours of a positive guiding example (e.g., must “yes” and “no” buttons have same the colour and contrast even if it’s a basic user-experience practice to give them different colours, thus enabling rather stifling choice?). Moreover, the

¹ *Digital Omnibus Regulation Proposal*, SWD (2025) 836 final, EUR. COMM’N (19 November 2025), <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>.

² *Joint Guidelines on the Interplay Between the Digital Markets Act and the General Data Protection Regulation*, EUR. COMM’N & EUR. DATA PROT. BOARD (9 October 2025), available at https://digital-markets-act.ec.europa.eu/document/download/8ba0913f-2778-4a6d-9c58-10f8c7ead009_en?filename=Joint_COM-EDPB_GLS_interplay_DMA_GDPR_for_public_consultation.pdf (hereinafter “Draft Joint Guidelines”).

³ Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743.

⁴ Draft Joint Guidelines, para 31.

⁵ Draft Joint Guidelines, para 42.

⁶ Draft Joint Guidelines, paras 40-45.

⁷ See Amanda Reid, Lorcan Neill, & Evan Ringel, *Nerd Harder: A Typology of Techno-Legal Solutionist Logics in Child Online Safety Laws*, POLICY + INTERNET (29 June 2025), <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.70012>.

section presents vague goals regarding user comprehension as a benchmark, merely paraphrasing the legal texts.⁸ In doing so, it fails to adopt a realistic assessment of users' level of interest and familiarity with legal frameworks like the DMA and GDPR.⁹

- The guidelines are unclear regarding separate consent requests for processing special category data under Article 5(2). They may be read as imposing a new disproportionate requirement to seek such consent, together with Article 5(2) DMA consent, even where there is no requirement to ask for it under the GDPR (*e.g.*, when the gatekeeper has already obtained consent).¹⁰
- The Draft Joint Guidelines acknowledge that users could be overwhelmed by a large number of requests from businesses for user-data portability under Article 6(10) DMA (“in particular where requests are repetitive or disruptive of the end user’s experience”).¹¹ Even with regard to obvious cases of abuse, however, the guidelines fail to state clearly that gatekeepers can protect users from “repetitive or disruptive” requests. Instead, they offer a vague statement about “layered and intuitive consent interfaces”, which does not address whether gatekeepers can refuse to convey some consent requests.

II. **Anti-Data Protection and Security Requirements (Articles 6(9) and 6(10) DMA)**

The DMA’s provisions on data portability, in Article 6(9) and 6(10), indisputably create data-protection and security risks. This is true not only for end users of DMA-regulated services, but also for any other person whose data happens to be in the user’s service account or—on the guidelines’ broad interpretation—even on the user’s device. These include *new* risks that users would neither expect, nor understand. Consider the following example.

A user, currently logged into a major social-networking service (the Gatekeeper), encounters a viral third-party application promising a “Digital Nostalgia” service. The application claims to use artificial intelligence (AI) to scan the user’s history and generate a sentimental video montage of their friendships. To initiate this process, the user is forwarded from the third-party website to the Gatekeeper’s authorization screen.

Because the user is already authenticated on the platform, they do not need to enter credentials; they are immediately presented with a standard consent popup. This popup bears the social network’s familiar and trusted branding. It lists the permissions the third-party app requires, which

⁸ Draft Joint Guidelines, para 45 (“Therefore, the choice presented to end users should not leave them unsure of how their data is processed or as to the degree of control they might have over their personal data under Article 5(2) DMA and the data protection rights conferred by the GDPR”).

⁹ On user rational disinterest (ignorance), *see, e.g.*, Daniel J. Gilman & Liad Wagman, *The Law and Economics of Privacy*, 29(2) UCLA J. L. & TECH. 55 (2024), available at https://laweconcenter.org/wp-content/uploads/2023/08/JOLT29-2_Gilman-Wagman.pdf.

¹⁰ Draft Joint Guidelines, para 37.

¹¹ Draft Joint Guidelines, para 172.

include access to historical photos—including images shared only with close friends or romantic partners—private message archives, and contact lists.

Crucially, the user sees only the Gatekeeper's familiar interface and instinctively applies the trust they have in that established platform to the unknown third party. The Gatekeeper's consent screen effectively launders the legitimacy of an unvetted requestor. Conditioned by years of “consent fatigue” from cookie banners and terms-of-service updates, the user performs a cursory scan of the permission list—indistinguishable from dozens of benign requests they have approved before—and clicks “Allow” to access the promised feature.

In that single instant, the nefarious application triggers the data-portability interfaces mandated by the DMA. This grants the third-party actor immediate access to a massive trove of sensitive historical data, allowing them to exfiltrate years of private correspondence and intimate media without further interaction from the user. The application need not even deliver the promised nostalgia video, although this may be helpful to attract more victims. The Gatekeeper's trusted UI effectively cloaks the risk of the unknown third-party requestor, creating a “Trojan Horse” effect where the ease of portability is weaponised against the user's privacy.

Under the requirement for “continuous and real-time” access, the threat extends beyond the user's historical data. By granting this permission, the user has inadvertently authorised a persistent data stream—effectively a “live wire” connected to their account. Even after the user closes the “Digital Nostalgia” tab and forgets the application exists—not having received any ongoing notification that data sharing continues (at least for months)—the third-party service retains a valid access token or webhook subscription. This allows the nefarious actor to instantaneously receive copies of every new private message sent, every new photo uploaded, and every location tag created. The user is under active surveillance, with their ongoing digital life being mirrored to a malicious server.

This asymmetry compounds the harm: a single click grants access, but revocation—if the user even remembers the application exists—can only break the link for future data. Any data already exfiltrated is, of course, already in the attacker's possession. The harvested information opens multiple vectors for exploitation: intimate images may be leveraged for sextortion; private messages mined for credentials, security questions, or blackmail material; and complete social graphs may be sold to data brokers, stalkers, or abusive ex-partners. All this stems from a single, momentary click on a consent form that took less time to approve than to read.

This textbook example of “consent phishing”¹² has some resemblance with the infamous Cambridge Analytica case.¹³ But much less information was available to Facebook apps like “This

¹² See, e.g., *Microsoft Delivers Comprehensive Solution to Battle Rise in Consent Phishing Emails*, MICROSOFT THREAT INTELLIGENCE (14 July 2021), <https://www.microsoft.com/en-us/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails>.

¹³ See, e.g., *Investigation into the Use of Data Analytics in Political Campaigns: A Report to Parliament*, INFO. COMM'R'S OFF. (6 November 2018), available at <https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.

Is Your Digital Life” in 2014-15 than would be under the DMA; importantly, there was no risk to private photos or messages. This is what is *new* about the risk: at a single click, an entire account and its most private contents could be sent to a third party (not to mention setting up ongoing surveillance).

Neither the European Commission, nor any other EU body, is currently conducting a public-information campaign to address this issue. This is despite the obvious fact that users of at least some DMA-regulated services have grown accustomed, with good reason, to trust that the manufacturer/service provider would not allow users to harm themselves so easily. But this is now possible under the DMA.¹⁴

Indeed, the Draft Joint Guidelines are generally dismissive of DMA-created risks to data protection and data security, which is surprising given the participation of the EDPB. Instead, they are preoccupied with interpreting the DMA’s explicit security and privacy provisions as narrowly as possible. The example detailed above illustrates two key problems with the guidelines:

1. They require gatekeepers *not to warn* users about clear and realistic risks of data portability; and
2. They prevent gatekeepers from excluding known bad actors as recipients of user data.

The guidelines state that “portability options and the wording used to describe them should be provided in a neutral and objective manner and should not nudge end users towards a specific choice”.¹⁵ In other words, they require gatekeepers to act as if every choice to port data—even a choice that would expose an entire service account (with private messages, etc.) or all data on a user device—is equally neutral and safe, which is obviously not the case.

Moreover, the guidelines explicitly forbid gatekeepers from restricting third parties’ receipt of user data—even when, *e.g.*, the third party has previously been fined or convicted for GDPR violations or is known to engage in practices like “consent phishing”. The Draft Joint Guidelines state:

Gatekeepers should also not gather information pertaining to the authorised third party’s compliance measures under the GDPR, including potential administrative or judicial proceedings the third party has undergone in relation to compliance with the GDPR, or whether the third party has suffered breaches of data security in the past.¹⁶

Gatekeepers would only be permitted to request “third parties’ identity details and information on whether, and to what extent’ the data to be ported” will involve transfers outside the EEA (to a country without an adequacy decision).¹⁷ The guidelines do not mention the possibility of

¹⁴ Mikolaj Barcentewicz, *The DMA’s Challenge to User Safety: Lessons from Apple’s Porn App Controversy*, TRUTH ON THE MKT. (4 February 2025), <https://truthonthemarket.com/2025/02/04/the-dmas-challenge-to-user-safety-lessons-from-apples-porn-app-controversy>.

¹⁵ Draft Joint Guidelines, para 126.

¹⁶ Draft Joint Guidelines, para 131.

¹⁷ Draft Joint Guidelines, para 130.

gatekeepers being allowed to verify whether such minimum information is even provided truthfully. In effect, gatekeepers are entirely disarmed from protecting users, even where they know the user is about to become a victim of consent phishing or another kind of attack.

The shortsightedness of this approach is especially staggering given the current geopolitical situation and well-known cyber operations of unfriendly states against the EU. The answer that the Draft Joint Guidelines provides to the issue of potential violations by third-party DMA beneficiaries is that such third parties are subject to the GDPR and potential GDPR enforcement (see the next section). Obviously, data-protection authorities will deter no criminal or state actor, and it is trivially easy to concoct front businesses putatively based in the EU, especially when gatekeepers are barred from verifying any information.

III. Prohibiting Gatekeepers from Implementing the Most Effective Measures for Data Protection and Cybersecurity

As noted above, according to the Draft Joint Guidelines, any privacy or security violations by DMA-beneficiary third parties can only be policed by actors other than the gatekeepers. The key problem with this approach is that gatekeepers are, in at least some cases, best placed to perform this oversight. Indeed, prevention is likely to be the only intervention that matters, especially in cases like data exfiltration through “consent phishing”.

Effective approaches are needed, because data protection and security are exceedingly difficult to police in practice—both in terms of deterrence and in terms of enforcement against violators. It simply cannot be credibly maintained that the mere fact that DMA’s beneficiaries are theoretically subject to the GDPR *solves* the issue of GDPR compliance. This is especially true for non-EU actors who aim to benefit from the DMA, either through legitimate but economically insignificant EU establishments, or by simply lying to gatekeepers about their identities.

In adopting this approach, the guidelines depart from previously stated Commission policy, supported directly by the DMA, that gatekeepers have a duty to ensure DMA implementation measures comply with other laws, including those on data protection and cybersecurity. For instance, Commissioner Margrethe Vestager stated in the European Parliament that:

It is for the companies to decide how will they present their services, their operating system, how will they make them safe for you and comply with the DMA.¹⁸

This aligns with Article 8(1) DMA, which states:

The gatekeeper shall ensure that the implementation of those measures complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC,

¹⁸ Committee on Internal Market and Consumer Protection Meeting, EUR. PARL. (3 April 2024), https://multimedia.europarl.europa.eu/en/webstreaming/event_20240403-0900-COMMITTEE-IMCO?start=240403071120&end=240403094524&audio=en; see also Mikolaj Barzentewicz, *Does the DMA Let Gatekeepers Protect Data Privacy and Security?*, TRUTH ON THE MKT. (4 April 2024), <https://truthonthemarket.com/2024/04/04/does-the-dma-let-gatekeepers-protect-data-privacy-and-security>.

legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements.

The guidelines note that,¹⁹ but add, in the context of Article 6(4):

At the same time, gatekeepers should not seek to instrumentalize their compliance with other applicable laws with a view to make their compliance with Article 6(4) DMA less effective. When selecting among several possible appropriate measures to comply with obligations stemming from other applicable laws, gatekeepers should select the measures that less adversely affect the pursuit of the objectives of Article 6(4) DMA, provided that they remain effective in ensuring compliance with those other applicable laws.

The legal interpretation implicit in this paragraph is highly questionable, as it appears to assume that DMA obligations take precedence over obligations from other EU legislation. One should ask whether the Draft Joint Guidelines apply the same logic to their interpretation of the DMA. In other words, when there are several ways to interpret the DMA and pursue its goals, do the guidelines choose those that less adversely affect pursuing other EU law objectives, including minimising restrictions of the rights protected by the EU Charter? Little in the Draft Joint Guidelines suggests that such balancing has been conducted, and that the guidelines are defensible from this perspective.

Setting this aside, Article 8(1) is entirely absent from the guidelines' section on the data-portability mandate under 6(10) DMA. The section on Article 6(9) references Article 8(1) in its discussion on authorised third parties, mentioning the GDPR's principle of integrity and confidentiality (Article 5(1)(f) GDPR) and the requirement to ensure the security of personal-data processing (Article 32 GDPR).²⁰ Notably, the principle of data minimization (Article 5(1)(c) GDPR) is not mentioned.

In that discussion, the Draft Joint Guidelines make the already-quoted point that gatekeepers should neither gather information on GDPR compliance by third parties wanting to benefit from the DMA, nor act on any information about their noncompliance. That point is followed by the following sentence:

Such information would not necessarily be an indicator of future compliance or the security of an application or related processing, and as such is not strictly necessary to comply with the gatekeeper's own responsibility under the GDPR.²¹

This reveals two important assumptions implicitly made in the guidelines, detailed in the next two subsections.

A. Gatekeepers Only Responsible for Own GDPR Compliance

First, Article 8(1) DMA concerns only "the gatekeeper's own responsibility under the GDPR". This is not the only possible reading of Article 8(1), and the guidelines provide no argument why this

¹⁹ Draft Joint Guidelines, para 88.

²⁰ Draft Joint Guidelines, para 129.

²¹ Draft Joint Guidelines, para 131.

reading should be adopted. On an alternative reading, which aligns with previous Commission policy as stated by Commissioner Vestager, gatekeepers are meant to ensure that DMA implementation measures comply with other laws, full stop.

In other words, it is the gatekeepers' responsibility to ensure—to the extent they can—that implementation measures do not lead to noncompliance with those other laws. It is true that gatekeepers cannot fully control, for instance, what third parties do with ported user data. But this does not mean that they should not at least implement technical and organisational measures (e.g., contractual measures) to safeguard compliance to the feasible extent. They are, after all, best placed to adopt such safeguards.

If gatekeepers do not do so, then DMA-created risks like the “consent phishing” example from the previous section will meet with no effective prevention. In other words, gatekeepers are the lowest-cost avoiders of harm.²² It is hard to argue that the aim of preventing them from performing a necessary service that they are best placed to do could be attributed to a rational choice by the EU legislature.

What is most puzzling is that the Draft Joint Guidelines do recognise this rather obvious point, but only in the section on search-engine data sharing under Article 6(11) DMA. There, the guidelines explicitly contemplate an implementing act that:

...may include an obligation for gatekeepers to contractually impose measures, where appropriate, on eligible third-party undertakings as a condition to access the data. Contractual requirements may, among others, limit onward sharing of the data received by eligible third-party undertakings. The implementing act may also impose specific monitoring obligations on the gatekeeper and also specify appropriate measures that gatekeepers must take in case of an established violation by third-party undertakings providing online search engines of requirements set out in the contract. Such measures may include requiring the gatekeeper to notify the competent data protection supervisory authority in case of an alleged breach of the GDPR, cease sharing data with the third-party undertaking providing an online search engine, and providing it with the contractual right to order the third party to delete any data it received from the gatekeeper.²³

We will return in the next section to this inconsistency in how the guidelines treat Article 6(11) and other provisions.

B. GDPR Applies Only to the Extent ‘Strictly Necessary’

The other revealed assumption in the Draft Joint Guidelines is that gatekeepers' responsibility under the GDPR should be interpreted narrowly, placing the DMA's goals above the GDPR's goals. The

²² By analogy with GUIDO CALABRESI, *THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS* (Yale University Press, 1970).

²³ Draft Joint Guidelines, para 189.

sentence from the guidelines cited above restricts the GDPR's application in a way that has no basis in the DMA: Gatekeepers are only allowed to comply with the GDPR to the extent this is "strictly necessary"²⁴. And not just "strictly necessary" as this is typically understood, but in some qualified, extreme sense.

In fact, it is hard to see the limiting principle of this restriction, given how facially unreasonable the provided example is. The guidelines state that, because it is *not always the case* ("would not necessarily be an indicator") that third parties' previous GDPR violations are predictive of future GDPR violations, *there can never be* a situation where prior violations indicate a strong likelihood of future violations. More precisely, there can never be a situation where knowledge of prior violations would permit a gatekeeper to better comply with the GDPR by refusing to transfer user personal data (likely including special categories of data) to such third parties. This is extremely surprising, given the EDPB's co-authorship of the guidelines.

As far as the DMA is concerned, it states that it applies "without prejudice" to the GDPR.²⁵ The DMA contains no general qualification that laws with respect to which it remains "without prejudice" apply only to the "strictly necessary" extent, much less in the extreme version suggested by the cited sentence.

IV. Inconsistent Interpretation of the DMA and the GDPR

As noted throughout this submission, the Draft Joint Guidelines adopt a restrictive interpretation of gatekeepers' ability to implement data-protection and security measures in the context of data portability under Articles 6(9) and 6(10) DMA. Gatekeepers are prohibited from gathering information about third parties' GDPR compliance history, from warning users about realistic risks, and from excluding known bad actors from receiving user data.

Yet the guidelines take a strikingly different approach when addressing search-engine data sharing under Article 6(11) DMA. There, the Draft Joint Guidelines appropriately recognise that data-protection risks require robust mitigation—even though Article 6(11) mandates that personal data be *anonymised* before sharing. The guidelines rightly acknowledge that anonymisation techniques may leave residual reidentification risks, depending on the means available to recipients and third parties. Of course, such risks should be primarily minimized by allowing gatekeepers to adopt state-of-the-art anonymization measures—the law requires nothing less than that.

To address these residual risks, the guidelines contemplate an implementing act that would:

- oblige gatekeepers to contractually impose measures on third-party undertakings as a condition of data access;
- limit onward sharing of received data;

²⁴ Draft Joint Guidelines, para 131.

²⁵ See, e.g., Recital 12.

- impose monitoring obligations on gatekeepers;
- require gatekeepers to notify competent data-protection authorities of alleged GDPR breaches (specifically, attempts to reidentify data);
- empower gatekeepers to cease sharing data with noncompliant third parties; and
- grant gatekeepers contractual rights to order third parties to delete any received data.

These are sensible and proportionate measures to address risks created by legally mandated sharing of personal data and may even in some cases be defensible in addressing risks related to data anonymized using state-of-the-art techniques. What is inexplicable is why the Draft Joint Guidelines do not apply the same logic—with at least equal force—to Articles 6(9) and 6(10), where the data transferred is *explicitly personal* and includes private messages, intimate photographs, and complete account histories.

The asymmetry cannot be justified on principled grounds. Both contexts involve transfers of data from gatekeepers to third parties. Both create risks that those third parties may violate the GDPR. Both involve situations where gatekeepers are best placed to prevent harm through technical and organisational measures. If anything, the case for robust protective measures is stronger under Articles 6(9) and 6(10), where there is no anonymisation requirement, and the data at stake is inherently more sensitive.

The “consent phishing” scenario we described earlier illustrates precisely why equivalent safeguards are needed: A single momentary click can expose an individual’s most intimate data to malicious actors, with no effective prevention mechanism if gatekeepers are prohibited from implementing protective measures.

We do not suggest that the measures contemplated under Article 6(11) are necessarily inappropriate—although they cannot be a substitute for robust anonymization. Rather, we urge the Commission and the EDPB to adopt a *consistent* approach across all DMA provisions involving the transfer of data to third parties. The principle that gatekeepers should serve as effective first-line defenders against data-protection violations—as the lowest-cost avoiders of harm—should apply uniformly throughout the DMA’s data-sharing provisions, and with no less rigour where actual personal data is at stake.

Absent such consistency, the Draft Joint Guidelines create a regulatory framework that is difficult to defend. It is one in which gatekeepers may monitor compliance and enforce contractual safeguards to protect against residual reidentification risks in anonymised search data but are forbidden from taking equivalent steps to protect users’ private messages and intimate photographs from known bad actors.

V. Omission of Interoperability Mandates (Article 6(7) DMA)

The Draft Joint Guidelines omit interoperability mandates under Article 6(7) DMA, incorrectly suggesting that such obligations come with no serious privacy issues, including questions about the interplay between the DMA and the GDPR, as well as the ePrivacy Directive.²⁶

In its Article 8(2) DMA decision from 19 March 2025 directed to Apple,²⁷ the Commission correctly noted that:

- “Article 6(7) of Regulation (EU) 2022/1925 shall be interpreted in conformity with the principle of proportionality and the fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union”²⁸.
- “... pursuant to Article 8(1) of Regulation 2022/1925, the gatekeeper shall ensure that the implementation of any measures pursuant to Article 6(7) of Regulation 2022/1925 complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cybersecurity, consumer protection, product safety, as well as with the accessibility requirements”²⁹.

In the same decision, however, the Commission appeared to ignore those points—including the third sentence of Article 8(1) DMA—and stated that “the measures that gatekeepers may introduce in relation to the interoperability solutions are limited to integrity measures”.³⁰ This statement requires, at the very least, robust justification, as it appears to contradict Article 6(7) DMA read not in isolation, but together with, *i.e.*, Article 8(1) third sentence.³¹

It is an appropriate subject for the Draft Joint Guidelines to explain how Article 6(7) DMA interplays with the GDPR (especially regarding virtual-assistant services that may be designated under the DMA) and with the ePrivacy Directive—particularly its Article 5(3).

²⁶ On privacy and security risks of interoperability mandates, *see, e.g.*, Mikołaj Barcentewicz, *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US* (TTLF Working Papers No. 84, Stanford-Vienna Transatlantic Technology Law Forum, 2022), <https://law.stanford.edu/publications/no-84-privacy-and-security-implications-of-regulation-of-digital-services-in-the-eu-and-in-the-us>.

²⁷ *Case DMA.100204, SP - Apple - Article 6(7) – Process*, EUR. COMM’N (19 March 2025), available at https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100204_2073.pdf.

²⁸ DMA.100204, para 85.

²⁹ DMA.100204, para 116 (similarly para 39).

³⁰ DMA.100204, para 40.

³¹ The remainder of the decision’s para 40 does not address the question of gatekeeper compliance with other laws under Article 8(1) third sentence when discharging their duties under Article 6(7). The paragraph merely lists how *other* DMA duties could interact with duties under other legislation.