Paul, Weiss

Client Memorandum

December 10, 2025

An Uncertain Journey on the Digital Omnibus: European Commission Takes Business-Friendly Step for Digital Regulation

On 19 November 2025, the European Commission (the "**Commission**") published a major package of proposed reforms to simplify and streamline digital regulation in the EU, including in relation to AI, privacy, data access and cybersecurity (the "**Digital Omnibus**"). [1] While the proposals are likely to evolve and be attenuated as they move through the legislative process, businesses operating in the EU's digital landscape should take note of potentially significant amendments to AI, data, privacy and cyber laws, including business-friendly amendments to the General Data Protection Regulation ("**GDPR**") and potential delays to the deadline for compliance with the EU AI Act (the "**AI Act**") for providers and deployers of high-risk systems. This alert focuses on the key changes proposed and practical takeaways if the legislation passes in its current form.

Key Takeaways

1. **Stop the clock for high-risk AI?** With widespread calls from industry to stop the clock on compliance obligations for high-risk AI systems until standards and guidelines are released, the Commission has proposed extending the timeline for providers and deployers of high-risk AI systems to comply, with a backstop of 2 December 2026 for Annex III systems (i.e. high risk sectoral activities) and 2 August 2028 for Annex I systems (product and safety components). However, the European Parliament and Council are still required to agree to these amendments and, given the slow process for legislation in the EU, any extension is likely to be last minute and businesses should continue rolling out compliance programs in advance of the current 2 August 2026 deadline.

2. **A pro-business shift, but don't count your chickens**. As a surprise, the suite of amendments to AI, privacy, data and cyber laws is very business-friendly, marking a departure from the EU's historical individual rights-based approach. This appears to be the result of extensive lobbying by businesses that digital regulation in the EU has gone too far in regulating businesses at the expense of innovation. Several of the proposed measures (including removal of AI literacy obligations and registration requirements for non-high-risk systems, exemptions for processing of special category data and clarified lawful bases for AI-related data processing, attenuated concepts of personal data and decreased transparency requirements) would undoubtedly simplify compliance and reduce administrative burdens. However, some of the proposed measures, particularly to data privacy laws, are likely to be considered fundamental in nature by lobbyists and will be subject to challenge. As such, there appears to be a low likelihood that all of these changes make it through the legislative process and, even if so, that they are not bogged down in EU court proceedings.

[1] Available here: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal and https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal.

© 2025 Paul, Weiss, Rifkind, Wharton & Garrison LLP. In some jurisdictions, this publication may be considered attorney advertising. Past representations are no guarantee of future outcomes.

Proposed Changes to the AI Act

1. **Delays to AI Act obligations**. To address the lack of harmonised standards and guidance under the AI Act, the Digital Omnibus suggests extending compliance deadlines for providers and deployers of 'high-risk' AI systems (i.e. those posing a significant risk to people's health, safety and fundamental rights) under the AI Act. The deadline would be extended from 2 August 2026 until the end of a six-month transition period (for Annex III systems used for in activities such as recruitment, emotion recognition and credit scoring) or a 12-month transition period (for Annex I products, or safety components of products, regulated under certain EU product safety laws) from the time that the Commission notifies that "adequate measures in support of compliance" such as harmonized standards are in place. These would then be subject to longstop dates of **2 December 2027** for Annex III systems and **2 August 2028** for Annex I systems. Additionally, a six-month grace period is proposed for providers of systems placed on the market prior to 2 August 2026 until **2 February 2027** to label AI-generated content.

2. **Attenuation of AI literacy obligations**. Responsibility is proposed to be shifted to the Commission and Member States to "encourage" literacy through non-binding measures like training and information resources, rather than requiring providers and deployers of AI systems to directly comply. Although training obligations on deployers of high-risk AI systems are to remain unchanged, the basis for the general amendment is unclear, especially given the relatively low burden it placed on providers and deployers in the first instance.

3. **Special category bias-detection exemption expanded**. The AI Act presently authorises *providers* of high-risk AI systems to process special category data for bias-detection, provided that no alternative data can achieve the same purpose, appropriate technical and organisational safeguards are implemented and the necessity of such processing is properly documented. The Digital Omnibus seeks to expand this exception by permitting both providers *and deployers* of *any* AI system, including high-risk systems, to process personal data for these purposes, subject to the same safeguards.

4. **Other simplification and pro-innovation measures**. The proposed amendments cover several other areas aimed at reducing administrative burdens on businesses, including (i) removal of the requirement to register AI systems determined not to be high-risk (e.g. when used for narrow procedural tasks), although with a right for the AI Office to still ask for a copy of the high risk analysis; (ii) removal of the requirement to rely on Commission templates for the preparation of post-market monitoring plans; (iii) expansion of the regulatory sandbox regime to provide for EU-level regulatory sandboxes for certain AI systems and extending the regulatory sandbox regime to cover high-risk systems covered by Annex I, section A of the AI Act; and (iv) extending regulatory simplifications (e.g. simplified technical documentation requirements and special consideration regarding penalties) to small mid-caps that were previously available only to SMEs.

Proposed Changes to Privacy and Cyber Regulation

1. **Streamlined incident reporting obligations**. One of the most welcome changes for businesses would be the "report once, share many" model proposed to be adopted for breaches and incidents under multiple legal acts including the Cyber Resilience Act, GDPR, NIS2 and DORA. Businesses would be able to notify authorities via a single entry point, reducing cost and administrative burden. Relatedly, the threshold for reporting data breaches would also be raised so as to require notification of personal data breaches only if it is likely to result in a *high* risk to data subjects' rights and freedoms and the time period for making such notifications is increased from 72 hours to 96 hours. The European Data Protection Board ("**EDPB**") would develop guidance on common breaches likely to result in a high risk.

2. **Revised definition of "personal data"**. The definition of personal data in Art. 4(1) of the GDPR would be clarified to reflect recent EU case law,[2] mandating a more subjective and context-specific approach to determining whether data is personal data. The assessment would centre on the perspective of the relevant controller, focusing on whether the relevant entity has "means reasonably likely to be used" to identify corresponding natural persons. This appears to be a significant step towards increased use of pseudonymisation and a more practical consideration of what data can be provided between businesses without triggering privacy compliance obligations.

3. **Lawful bases for AI training**. Processing personal data for the purpose of developing and training AI systems could be justified on the basis of legitimate interests. However, this is subject to notable exceptions, namely where EU or national

[2] See *European Data Protection Supervisor v Single Resolution Board (C-413/23 P)*, available here: https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=16466915

laws require consent, and subject to appropriate technical and organisational safeguards, including an unconditional right for data subjects to object. As is currently the case, there must also be a balancing of the controller's interests with those of the data subject. Notably, if the data subject is a child, legitimate interests may not be used as a lawful basis for processing their special category data. Two additional exemptions from the prohibition on processing special categories of personal data would also be introduced for: (i) processing special category data to develop and operate AI systems where residual special category data remains despite implementing appropriate technical and organisational measures to avoid such collection (with such circumstances being an express legal basis for such processing); and (ii) biometric data for identity verification when the data or means needed for verification are under the control of the data subject (the proposal does not specify whether such verification needs to be initiated by the data subject).

4. **Other simplifications of privacy laws**. There are a significant number of other amendments proposed to the GDPR, the equivalent version of the GDPR that applies to public bodies, the e-Privacy Directive, the Data Act and other privacy and cybersecurity laws, which are generally made with an aim to ease the compliance burden for businesses and improve user experience. The key proposals are: (i) a prohibition on data localisation requirements for non-personal data under the Data Act; (ii) the creation of a European Data Innovation Board, including representatives from member states, the EDPB and other regulatory bodies, as a forum to discuss data policies, governance, international flows and cross-sectoral developments and foster cooperation between authorities; (iii) updates to the cookies consent framework to remove the consent requirement for first-party cookies to create aggregated usage information for the controller's own use and, where consent is required, a requirement for the ability to reject cookies with one click; (iv) the ability for controllers to refuse (or charge a fee to comply with) subject access requests made "*for purposes other than the protection of [data subject's] data*"; and (v) a right for controllers not to provide transparency information to data subjects upon collection where the relationship between them is not data-intensive, there are reasonable grounds to assume the data subject already has the information and certain other activities are not taken (e.g. transfer to a third country or automated decision marking) – this appears to apply to circumstances where, for example, personal data is taken from a website such as LinkedIn.

Comment

The Digital Omnibus is a set of proposals only. It is likely to be subject to potentially significant change as it progresses through the legislative process, requiring approval by both the European Parliament and the Council of the EU. In addition, the Commission will also carry out a Digital Fitness Check[3], open until 11 March 2026, to examine the coherence and cumulative impact of the EU's digital rules. By including such wide-ranging amendments in one instrument, the Commission has set an ambitious goal of agreeing all of these amendments before 2 August 2026, when existing high-risk AI obligations under the AI Act otherwise come into effect. Whether this deadline is met, which amendments are approved, and what happens if the deadline is not met, remains to be seen.

Additionally, although many of these changes appear sensible on their face and will likely be welcome to businesses and consumers alike, it is unlikely that the EU's very active lobbyist groups will not put up a fight. Certainty on any agreed legislative changes is unlikely to be clear for a number of years.

For now, AI developers should continue to develop compliance frameworks with the current legislation (and deadlines) in mind, but the Digital Omnibus proposals are an important reminder of the need for flexibility as businesses navigate a fast-changing technological and regulatory landscape. The EU appears to be looking at its friends in the US and UK and realising that, to stay relevant in a global economy, it needs to move back from its stringently pro-individual rights stance.

[3] Details here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Katherine B. Forrest
+1-212-373-3195
kforrest@paulweiss.com

Nicole Kar
+44-20-7601- 8657
nkar@paulweiss.com

Henrik Morch
+32-2-884-0802
hmorch@paulweiss.com

John Patten
+44-20-7367-1684
jpatten@paulweiss.com

Georgina Hoy
+44-20-7601-8743
ghoy@paulweiss.com

Alex Zapalowski
+44-20-7367-1697
azapalowski@paulweiss.com

Associate Ali Fazeli-Nia contributed to this Client Memorandum.