Matheson | CELEBRATING 200 YEARS

EU Digital Omnibus Regulations – What has been proposed?

Author: Davinia Brennan
Co-Authors: Marie McGinley, Sarah Jayne Hanna, Anne-Marie Bohan
With special thanks to Ben Doyle and Susan Fitzharris for their contribution to this article

Introduction

On 19 November 2025, the European Commission published its draft Digital Omnibus Regulations (EU Regulations 2025/0360 and 2025/0359). The proposed reforms set out in the two legislative proposals come as a result of the Draghi and Letta reports in 2024, which aim to introduce greater competition through innovation and efficiency within the EU. They seek to simplify the EU's digital laws, cut compliance costs for companies across the EU, and help start-ups to grow without facing unnecessary red tape.

EU Regulation 2025/0360 proposes amendments to: the Data Act, GDPR, the ePrivacy Directive and NIS2. It will also consolidate the Free Flow of Non-Personal Data Regulation, the Open Data Directive and the Data Governance Act into a single piece of legislation, namely the Data Act, to ensure the legislative instruments are better aligned, aiming to enhance legal clarity and consistency. In addition, the Platform to Business ("**P2B**") Regulation will be repealed, as its objectives are now largely covered by the Digital Markets Act and the Digital Services Act. Meanwhile, EU Regulation 2025/0359 proposes amendments to the AI Act.

Key Changes proposed by the draft Digital Omnibus on AI (2025/0359)

AI Act

The AI Act (EU Regulation 2024/1689) entered into force on 13 June 2024 and is coming into force on a phased basis, with most provisions due to be implemented by 2 August 2026. Stakeholder consultations throughout 2025 revealed implementation challenges that need to be addressed so that the AI Act can be successfully rolled out.

The proposed amendments including the following:

- **Timeline changes for high-risk AI systems (amending Article 113, AI Act).** It is proposed that the applicable date for the entry into application of the obligations for providers and deployers of high-risk AI systems should be delayed by a maximum of 16 months, to align with the availability of support tools, including the necessary technical standards.

  The entry into application of the rules governing high-risk AI systems pursuant to Article 6(2) and Annex III, and those high-risk AI systems pursuant to Article 6(1) and Annex I, is delayed by six months and twelve months respectively, following approval of corresponding technical standards. However, this flexibility should only be extended until 2 December 2027 for those high-risk AI systems in Article 6(2) and Annex III, and 2 August 2028 for those covered by Article 6(1) and Annex I.

- **Timeline change for transparency obligation (amending Article 111, AI Act).** A six-month grace period is proposed in respect of the transparency obligations in Article 50(2) of the AI Act, for those who have already placed their systems on the market before 2 August 2026. This is to allow sufficient time for providers of generative AI systems subject to marking obligations to adapt their practices within a reasonable time without disrupting the market.

- **Reduced AI literacy obligations (amending Article 4, AI Act).** Rather than requiring providers and deployers to implement AI literacy, it is proposed that the European Commission and Member States should instead foster AI literacy, and "encourage" providers and deployers of AI systems to take measures to ensure a sufficient level of AI literacy. This amendment is proposed following feedback from stakeholders that there is no one-size-fits-all solution available in respect of the promotion of AI literacy, rendering a horizontal obligation ineffective in achieving the objective pursued by this provision.
- **Legal Basis to process limited amounts of special category data (new Article 4a, replacing Article 10(5), AI Act).** Introduction of a new provision which provides a legal basis for providers and deployers of AI systems and AI models to exceptionally process special categories of personal data for the purpose of ensuring bias detection and correction under certain conditions.
- **Simplified procedures for designation and conformity of notified bodies (amending Article 28, AI Act).** These procedures include a single application and assessment procedure, and requirements for conformity assessment bodies applying to be designated as notified bodies, to do so with reference to a new list of codes.
- **Strengthening of AI regulatory sandboxes (amending Articles 57, 58 and 60, new Article 60a, AI Act).** Introduction of procedural simplification and clarity in governance of regulatory sandboxes and increased scope for real world testing of high-risk AI systems outside of regulatory sandboxes.
- **Enhanced role for the AI office (amending Article 75, AI Act).** It is proposed that the AI Office should have increased powers in relation to the monitoring and supervision of certain AI systems based on general purpose AI models (where the model and system is developed by the same provider). It provides therefore that the European Commission should be empowered to adopt implementing acts to specify those powers of the AI Office, including the ability to impose administrative fines and other sanctions, in accordance with the conditions and ceilings identified in Article 99 of the AI Act.
- **Removal of certain EU database registration requirements (repeal of Article 49(2), AI Act).** Providers of AI systems referred to in Article 6(3) (i.e. AI systems used in high risk areas listed in Annex III, but which the provider has concluded do not pose a significant harm to health, safety or fundamental rights), are not required to register such systems in the EU database. In such circumstances, it is considered by the European Commission that registration would cause a disproportionate compliance burden.
- **Extension of some SME regulatory privileges to SMCs (amending Article 99 and Article 1, AI Act).** It is proposed that existing regulatory privileges in Article 99 afforded to small and medium-sized enterprises ("**SMEs**") should be extended to small mid-cap enterprises ("**SMCs**"), with the result that smaller and more proportionate penalties (such as fines and other administrative sanctions), may be imposed on SMCs. In addition SMEs and SMCs will benefit from simplified technical documentation requirements.

Key Changes proposed by the draft Digital Omnibus (2025/0360)

NIS2

NIS2 (Directive 2022/2555) will be amended to establish a single-entry point for a series of incident reporting obligations under various data protection and cybersecurity instruments (inserting a new Article 23a NIS2). The aim of this proposal is to create a simplified, harmonised process for incident reporting across the EU, bringing high costs savings for businesses. The proposal notes that through fostering the "report once, share many" principle, this will reduce the administrative burden for entities, while ensuring effective and secure reporting of security.

Article 23a NIS2 requires the EU's cybersecurity agency, ENISA, to develop and maintain the single-entry reporting point for companies to report security incidents and related events to a single interface, in order to fulfil their obligations under all applicable EU legislation, including NIS2, GDPR (EU Regulation 2016/679), DORA (EU Regulation 2022/2554), eIDAS Regulation (EU Regulation 910/2014), and the CER (EU Directive 2022/2557).

GDPR

The GDPR (EU Regulation 2016/679) will also be simplified. Whilst stakeholders have generally found the GDPR to be fit for purpose, some organisations, especially smaller entities with low-risk data processing operations, have raised concerns regarding certain obligations. The amendments aim to address these concerns.

The proposed amendments to the GDPR include:

- **Subjective approach to the definition of "personal data" (amending Article 4(1) GDPR).** The mere fact that another entity may be able to identify a data subject will not make that information "personal data" in the hands of the current holder. The definition of "personal data" will be clarified to state that information is not to be considered personal data for a given entity when it does not have means reasonably likely to be used to identify the natural person to whom the information relates. The proposed definition is in line with the recent CJEU ruling in Case C-413/23 P, EDPS v SRB.
- **Additional exemptions to the processing of "special category data" (amending Article 9(2) GDPR).** Two additional exemptions to the prohibition on the processing of special category data are also proposed. Firstly, allowing the processing of biometric data when necessary to confirm the identity of the data subject and when the data and means for such verification are under the sole control of that data subject. Secondly, allowing the residual processing of special category data for development and operation of an AI system or AI model, subject to certain conditions, including appropriate organisational and technical measures to avoid collecting special category data and removing such data.

- **New definition of "scientific research" (new Article 4(1)(38) GDPR).** A definition of scientific research is proposed. It includes *"any research which can also support innovation, such as technological development and demonstration…"*. In addition, the amendments clarify that further processing for scientific purposes is compatible with the initial purpose of processing, and that the processing of personal data for scientific research purposes constitutes a legitimate interest within the meaning of Article 6(1)(f) GDPR (provided such research is not contrary to EU or Member State law).
- **Clarification of scope of "manifestly unfounded or excessive" exemption to data subjects' rights (amending Article 12(5) GDPR).** Clarification as to when a data subject request amounts to an abuse of law and exploitation of their data protection rights, and hence constitutes a "manifestly unfounded or excessive" request is proposed. In such situations a controller may refuse to comply with the request or charge a reasonable fee. This amendment is aimed at alleviating the burden of responding to data subject requests, in particular access requests. These requests can cause significant disruption to a controller's business, and frequently occur in the context of contentious employment disputes.
- **Data privacy notices not required where data subjects already have the relevant information (amending Article 13(4) GDPR).** This amendment would remove the obligation to inform data subjects (via a data privacy notice) about the processing of their personal data under Article 13 GDPR, in situations where there are reasonable grounds to assume that the data subject already has the information. However, this exemption would not apply in circumstances where the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, or the processing is likely to cause a high risk to data subject's rights.
- **Clarification of scope of automated decision-making (amending Article 22 GDPR).** A minor amendment is proposed to Article 22 GDPR to clarify the requirements for automated decision-making in the context of entering into, or performance of, a contract between a data subject and a controller. In particular, it is clarified that the requirement of "necessity" is regardless of whether the decision could be taken otherwise than by solely automated means.
- **Higher threshold and time-limit for reporting data breaches to DPAs and single-entry reporting point (amending Article 33 GDPR).** It is proposed that the threshold for reporting personal data breaches to data protection authorities would be raised, so that only incidents posing a "high risk" to data subjects would be reported. This aligns with the current threshold for reporting personal data breaches to data subjects under Article 34 GDPR. In addition, the period for reporting would be extended from 72 hours to 96 hours.

  It is further proposed that controllers should use the single-entry reporting point when they notify data breaches to the supervisory authority. In addition, the European Data Protection Board ("**EDPB**") would be obliged to prepare and submit to the European Commission a proposal for a common template for data breach notifications, which the Commission would be empowered to adopt by means of an implementing act, after reviewing it, as necessary.

- **Harmonisation of processing activities requiring a DPIA (amending Article 35 (4)-(6) GDPR).** The EDPB will set out a list of processing activities where a data protection impact assessment ("**DPIA**") is required and is not required, thereby contributing to the harmonisation of the notion of "high risk" under Article 35 GDPR. In addition, the EDPB will be obliged to introduce a common template and common methodology for conducting a DPIA, which the European Commission would be empowered to adopt by means of an implementing act, after reviewing them, as necessary.
- **Processing of personal data for AI training purposes is a legitimate interest (inserting a new Article 88c GDPR).** A new GDPR provision would confirm that processing personal data for model training is a legitimate interest under Article 6(1)(f) GDPR. A balancing test must, however, be carried out to ensure such processing is necessary and not overridden by the interests or fundamental rights and freedoms of the data subject.
- **Cookie consent (inserting a new Article 88a GDPR).** A new GDPR provision would set out the consent requirement (currently part of the ePrivacy Directive) for the storing or accessing of personal data on the terminal equipment of individuals, and bring the processing of personal data on and from terminal equipment within the rules of the GDPR.

  In addition, individuals must be able to refuse all cookies with a "single-click button". Cookie banners will need to make this possible by including a single-click button. Websites must respect individuals' choices for at least six months.

  Article 88a GDPR would also extend the two exemptions from consent requirements that currently exist, namely, cookies used (i) to provide a user-requested service or (ii) to transmit a network communication. Two further exemptions are proposed in respect of cookies used for (iii) aggregated analytics purposes and (iv) security purposes. In addition, Article 88a allows cookies to be deployed under any lawful basis under Article 6 GDPR, not just consent, at least in so far as necessary to "safeguard the objectives set out in Article 23(1)".
- **Automated and machine-readable indications of data subjects' choices with respect to the processing of personal data in their terminal equipment (inserting a new Article 88b GDPR).** A new GDPR provision provides for automated and machine-readable indications of individual choices (i.e. either consent or objection) in respect of those indications by website providers once standards are available. Standards bodies would be instructed to develop benchmarks for machine-readable signals. The goal here is to enable individuals to set their privacy preferences centrally, for example via the browser, and websites must respect them. This will alleviate consent fatigue and simplify users' online experience.
- **Support with assessing whether data resulting from pseudonymisation does not constitute personal data (inserting a new Article 41a GDPR).** It is proposed that the European Commission may adopt implementing acts to help controllers assess whether data resulting from pseudonymisation no longer constitutes personal data. The implementing act will outline the means and criteria relevant for such an assessment, including the state of the art of available techniques and criteria to assess the risk of reidentification.

e-Privacy Directive

As mentioned above (in respect of the new Articles 88a and 88b GDPR), it is proposed that the e-Privacy Directive (Directive 2002/58/EC) would be amended to provide a regulatory solution to "consent fatigue" and the proliferation of cookies banners, which the European Commission recognises as "long-overdue".

The proposals also include:

- **Repeal of breach reporting requirements (repeal of Article 4, e-Privacy Directive).** The personal data breach reporting obligations for communications service providers under this provision would be repealed on the basis that they are obsolete in view of the breach reporting obligations under the GDPR.
- **Moving the cookie rules, in respect of the processing of personal data, to the GDPR (amending Article 5(3), e-Privacy Directive).** It is proposed that Article 5(3) ePrivacy Directive would be disapplied in respect of the storing and accessing of "personal data" from the terminal equipment of a natural person. In this case, the new Article 88a GDPR would apply instead.

Data Act

The Data Act (EU Regulation 2023/2854) entered partly into force on 12 September 2025, with the remaining chapters due to enter into force on 12 September 2027. The amendments proposed to the Data Act aim to boost legal clarity around that legislation and drive competitiveness. They also recognise an urgent need to strengthen safeguards against the risk of trade secret leaks to third countries, and to alleviate the regulatory burden for SMEs and SMCs.

The proposals regarding the Data Act include:

- **Consolidation of three existing EU legislative instruments,** including (i) the Data Governance Act (EU Regulation 2022/868), (ii) the Free Flow of Non-Personal Data Regulation (EU Regulation 2018/1807) and (iii) the Open Data Directive (EU Directive 2019/1024) into the Data Act. This consolidation aims to establish a unified rulebook for how data held by public authorities can be reused, eliminating overlapping and contradictory provisions, and enhancing legal certainty.
- **Switching obligations for data processing services (amending Article 31, Data Act).** It is proposed that switching obligations for data processing services are adjusted for custom made services and for SMEs/SMCs with legacy contracts concluded before 12 September 2025, while preserving the goal of eliminating switching and egress charges. Providers can include proportionate early termination penalties, but not barriers to switching.
- **Repeal of "smart contracts" essential requirements (deletion of Article 36, Data Act).** It is proposed that Article 36 of the Data Act is deleted. That provision sets out essential requirements for smart contracts used in data-sharing arrangements without replacement.

- **Removal of mandatory registration for data intermediation service providers (amending Article 32, Data Act).** It is proposed that the European Commission would maintain a public EU register listing recognised data intermediation service providers and recognised data altruism organisations, creating transparency and helping businesses identify reliable partners in the data-sharing ecosystem.
- **Strengthened protection for trade secrets (amending Article 4(8) and 5(11), Data Act).** Trade secret holders may refuse requests for the disclosure of trade secret data, where such disclosure would result in serious economic damage for the data holder. A data holder may also refuse to disclose a trade secret where such disclosure is to entities located in third countries, particularly where those third country legal regimes offer weaker protection than the EU. The refusal must be based on a case-by-case assessment of all objective factors.
- **Further restriction of access to data by public authorities (inserting a new Article 15a, Data Act).** It is proposed that the circumstances under which public authorities can demand data from businesses should be significantly narrowed from "exceptional need" to "public emergencies". Data holders would only be required to make certain data available to public sector bodies, where genuinely necessary to respond to a public emergency or to help mitigate or recover from one. Microenterprises and small businesses would gain the right to seek compensation when required to provide data during emergencies. However, larger data holders would continue to provide data without charge in these emergency situations.

Comment

The legislative changes proposed by the draft Digital Omnibus Regulations aim to streamline and simplify the rules on AI, cybersecurity and data, and ease companies' compliance efforts. In addition, the proposed adjustment of the time-line for applying high-risk AI rules to a maximum of 16 months would mean that the rules start applying once the much needed standards and support tools are available. However, it remains to be seen whether the draft Regulations will be adopted before the high-risk AI system rules are due to come into force in August 2026.

The draft Digital Omnibus Regulations will now be submitted to the European Parliament and the Council for adoption, and will inevitably be subject to intense trilogue negotiations over the coming months. We will monitor these negotiations closely, and keep you updated, as you will need to take steps to ensure that your data protection, ICT and AI systems comply with the above changes to the extent that they are adopted.

Contact Us

Matheson's Technology & Innovation Group are available to guide you through the proposed reforms set out in the draft Digital Omnibus Regulations, and related legislation. For more information, please contact any member of our Technology and Innovation Group or your usual Matheson contact.

Davinia Brennan
Partner
T +353 1 232 2700
E davinia.brennan@matheson.com

Anne-Marie Bohan
Partner
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Sarah Jayne Hanna
Partner
T +353 1 232 2865
E sarahjayne.hanna@matheson.com

Marie McGinley
Partner
T +353 86 170 650
E marie.mcginley@matheson.com

Matheson | CELEBRATING 200 YEARS

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock,
Cork, T23KW81
Ireland

T: +353 21 465 8200
E: cork@matheson.com

LONDON
7th Floor, Octagon Point,
5 Cheapside,
London EC2V 6AA,
UK

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
250 Park Avenue
New York,
NY 10177
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
228 Hamilton Avenue,
3rd Floor,
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
95 Third Street
San Francisco
CA 94103
United States

T: +1 415 423 0540
E: sf@matheson.com