Data Protection and the EU's Digital Omnibus Package

Author: Steven Roberts, CDIR CDPO is a Certified Data Protection Officer, Chartered Director and Vice Chair of the Compliance Institute's Data Protection & Information Security Working Group.

Recent years have seen an increasing divergence in the regulatory approaches of the EU and the US. The former has introduced new legislation in areas such as cybersecurity, data governance and artificial intelligence (AI), as part of its Digital Decade initiative. The US administration, by contrast, has focused on reducing regulation to encourage economic growth and innovation, particularly in areas such as AI.

In 2024, the EU commissioned Mario Draghi to examine how EU competitiveness could be improved. His report on *The Future of European Competitiveness* identified increased regulation as a significant barrier to growth. Draghi noted ***'We claim to favour innovation, but we continue to add regulatory burdens onto European companies'.***

In November 2025, the EU published a proposed suite of changes to existing legislation, known as the EU Digital Omnibus Package[1]. Intended as a 'mid-course correction', it seeks to amend existing EU laws (including the GDPR) to reduce and simplify the regulatory burden, especially for SMEs, streamline reporting and provide greater harmonisation.

Redefining Personal Data

The Omnibus introduces a revised definition of personal data. Under the proposal, information would only be considered as personal data if the organisation is reasonably likely to be able to identify the individual. In addition, pseudonymized information would no longer be considered personal data where it is held by an entity that does not have the tools or resources to reidentify the data subjects.

Artificial Intelligence and Data Processing

A number of new provisions are intended to provide greater clarity where personal data is processed by AI technologies. For example, to recognize as a legitimate interest the use of personal data for the development and operation of AI systems. The Omnibus also proposes limited exceptions that would allow for the processing of special category data in the development of AI; for example, as part of bias detection. This would be subject to strict safeguards.

Reporting and Operations

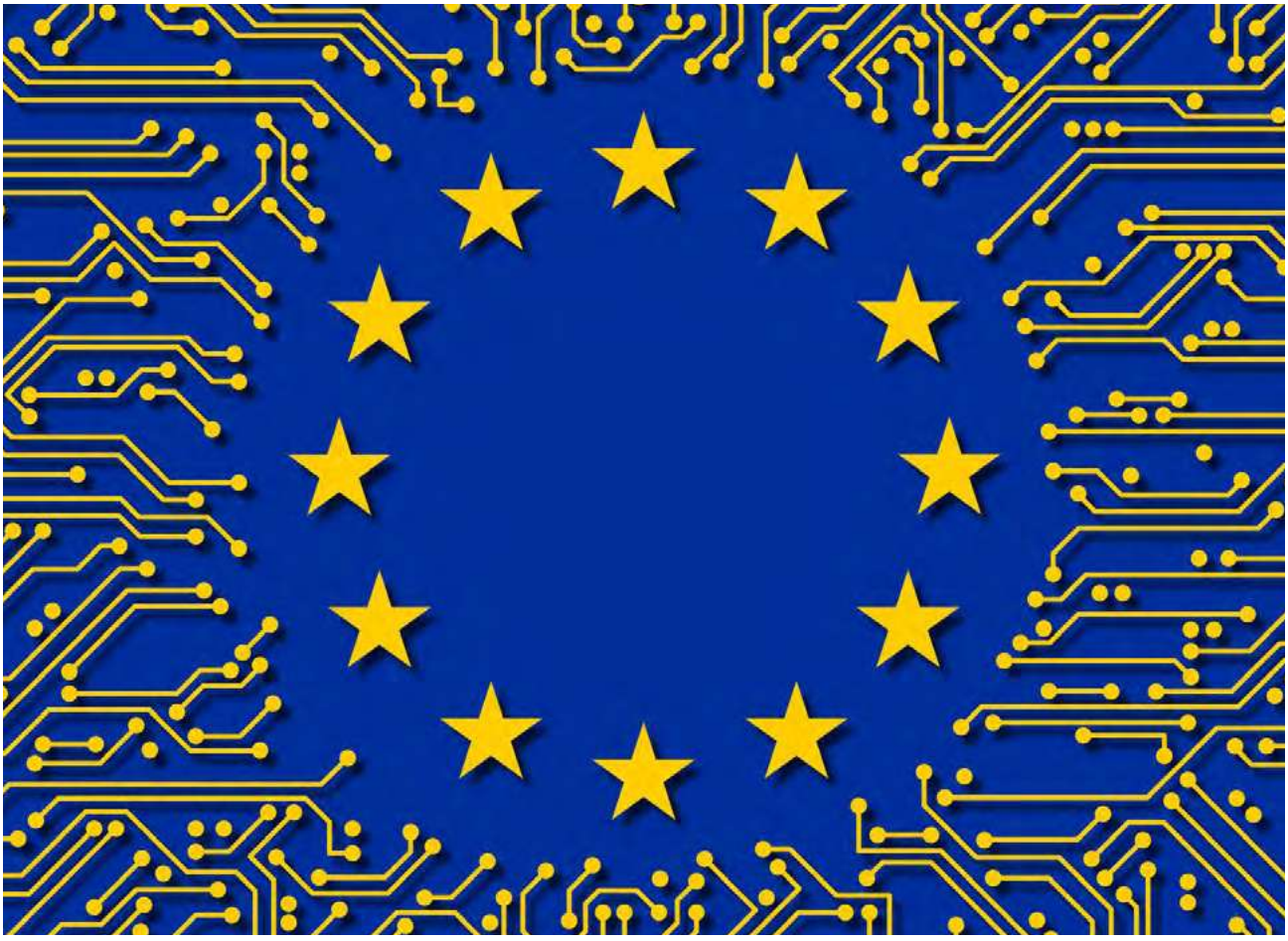
The reporting threshold for notifying the Data Protection Commission or other relevant supervisory authorities would be amended to include only those breaches that pose a high risk to individuals. The reporting deadline would also be extended from 72 hours to 96 hours. Both would be welcome developments for companies, particularly smaller firms with fewer compliance resources.

The European Data Protection Board (EDPB) would be tasked with developing a standardized notification template and a list of circumstances where a breach is likely to result in a high risk to individuals. This would be reviewed and updated accordingly at minimum every three years.

The EDPB would compile at EU-level a listing of processing operations that require completion of a Data Protection Impact Assessment (DPIA), replacing the current regime where each national authority provides its own list[2].

1 The Omnibus package includes two legislative components - one focused specifically on AI and one focused on data, privacy and cybersecurity.

2 The EDPB recently undertook a public consultation on a proposed DPIA. Template that could be adopted by EU supervisory authorities or used as a "meta-template' with which national specific templates will be compatible'. For further information, see: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en.



A new, single-entry reporting portal would be introduced to allow organisations submit a single report to fulfil obligations under a range of EU legislation, including DORA, GDPR, NIS2, the Cyber Resilience Act, and others.

Cookie Reform

The decision in 2025 to indefinitely pause the proposed ePrivacy Regulation was unwelcome news for companies, particularly those operating across EU member states. Under the Omnibus, it is proposed that consent requirements for cookie banners would be placed under the GDPR.

In an effort to reduce cookie fatigue and counteract nudge techniques on websites, a single-click refusal or 'reject all' button would be required on cookie banners; this should be as simple to select as the 'accept all' option.

Where a user refused consent, companies would have a six-month moratorium before they could make a new consent request for the same processing purpose. Data controllers would also be required to accept machine-readable data, such as browser-level privacy settings, once the technical standards had been established.

In certain limited circumstances, cookies would not be required to create aggregated data for audience measurement or for the maintenance or restoration of website security. However, it is unlikely that commonly-used tracking and analytics tools that operate across platforms would come within the scope of this exemption.

Data Subject Rights

One of the more notable changes would enable controllers to refuse to act on a Data Subject Access Request (DSAR), or charge a fee, where the organisation has reasonable grounds that the request is an abuse of rights or has been made for purposes other than the protection of personal data.

Restrictions on automated decision-making under Article 22 would be reduced to permit such processing where necessary for entering into or performing a contract.

Privacy notices will not be required where the use of personal data is low risk and the organisation has reasonable grounds to expect the data subject already knows who the data controller is and the legal basis for why the processing is taking place. This exemption would not cover aspects such as international data transfers, automated decision-making or where other high-risk processing takes place.

Small and Mid-Cap Enterprises

The Omnibus recognises a new category of company, known as small mid-cap enterprises or SMCs. These are organisations with fewer than 750 employees, annual turnover of up to €150 million and total assets of up to €129 million. Mitigations currently available to small-to-medium sized companies under the GDPR, such as the exemption from maintaining a Record of Processing Activity (RoPA) in certain circumstances, would be extended to this new SMC category.

Subject to Change

It is important to note that these and other changes under the Omnibus are currently only at the proposal stage and have yet to be ratified within the EU's trilogue process. There may be substantial changes to some or all of the proposed amendments. The AI and Data components within the overall Omnibus package are proceeding along separate timelines; at present, it is unlikely the Data element will be finalised before early 2027.

The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) have already noted significant concerns. In a joint opinion adopted in February, they stated the proposal could 'adversely affect the level of protection enjoyed by individuals, create legal uncertainty and make data protection law more difficult to apply'. It is likely that lobbying will continue throughout the year by those seeking lighter regulation and those seeking to maintain the existing level of safeguards.

It is to be hoped that certainty is provided sooner than later. Whilst a reduction in regulatory requirements is broadly positive, the current lack of clarity is confusing and destabilising for businesses and counteracts the very purpose the Omnibus seeks to achieve.

What steps can organisations take to prepare for the Omnibus?

There are some practical measures organisations can take.

1. Keep the Omnibus as a standing agenda item throughout the year to maintain visibility.
2. Maintain ongoing engagement with key stakeholders. Effective planning and implementation will require cross-functional collaboration within the organisation.
3. Ensure a team member is identified to keep updated on any further proposed developments or changes to the Omnibus.
4. Identify which existing data protection and broader compliance processes would be most impacted by the proposed changes.
5. Pay particular attention to any announcements from the Data Protection Commission (DPC) on proposed timelines for introduction.
6. Ensure that senior management and staff at all levels of the organisation are aware the Omnibus is only a proposal and that, as per currently, there are no material changes to Europe's data protection regime.
7. Keep some contingency within the annual plan of work to ensure resource is available if the Omnibus package is introduced within the next 12 to 18 months.

Compliance Institute members seeking further information on the Digital Omnibus are encouraged to view the Institute's recent CPD webinar on this topic, which is available on Compliance.ie. A Compliance Files podcast on the Omnibus is also scheduled for the coming months.

About the Author: Steven Roberts CDIR CDPO is a Certified Data Protection Officer, Chartered Director and Vice Chair of the Compliance Institute's Data Protection & Information Security Working Group. His new book, ***Data Protection for Business: Compliance, Governance, Reputation and Trust,*** is published by Clarus Press.