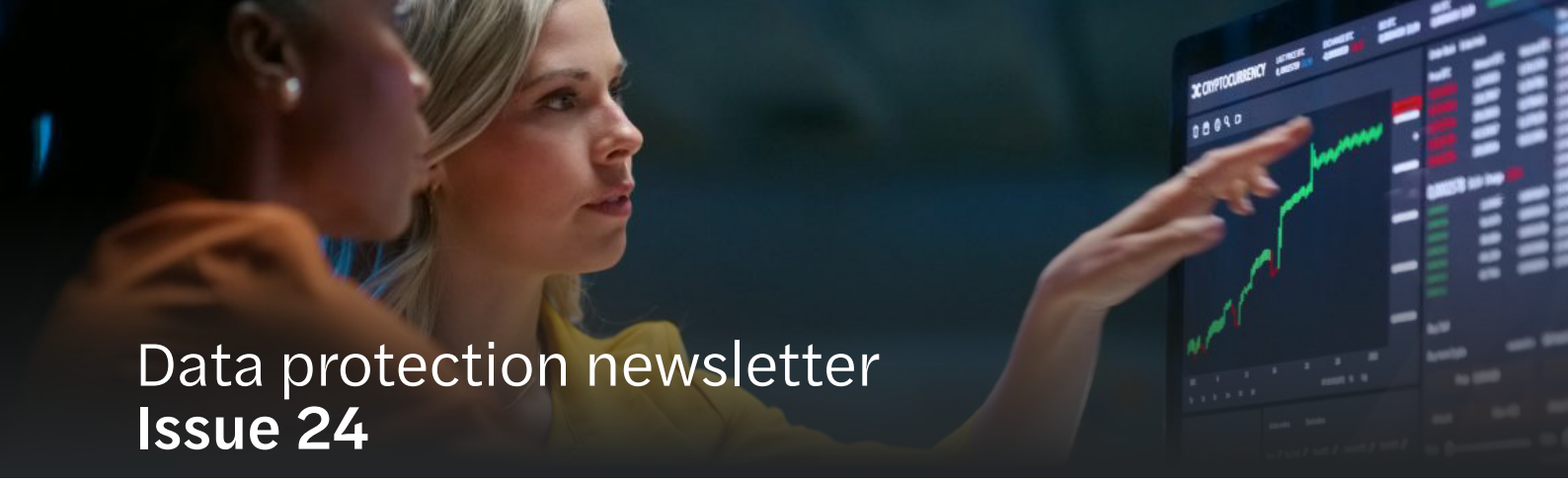

Data protection newsletter
Issue 24

In this issue, we explore a number of significant developments shaping the privacy and regulatory landscape across Europe and beyond. We examine emerging challenges for international data transfers, including the potential implications of the US Supreme Court's decision in Trump v. Slaughter for the EU-US Data Privacy Framework, and the European Data Protection Board's approval of GDPR certification as a new transfer mechanism.

We also look at continued regulatory scrutiny of data-driven marketing practices, following a major enforcement action by the Norwegian Data Protection Authority concerning social media-based advertising and consent practices. In addition, we review recent Irish Data Protection Commission fines issued to the HSE and Permanent TSB, highlighting key lessons on security, governance and breach notification obligations.

Finally, we provide an update on the European Commission's proposed Digital Omnibus package and its potential impact on the implementation of the EU AI Act, including changes to compliance timelines, transparency requirements and obligations for organisations deploying AI systems.

As regulators continue to focus on accountability, transparency and safeguarding personal data, organisations should closely monitor these developments and assess whether any changes are required to their data protection and AI governance frameworks.

International transfers

Trump v Slaughter – Impact on EU-US Data Protection Framework

Background

Upon taking office in 2025, President Trump sought to dismiss Slaughter from her position of commissioner at the Federal Trade Commission (FTC). Slaughter challenged her dismissal as a previous court ruling had found that US Presidents could not dismiss commissioners of independent agencies, such as the FTC, without cause. The case was eventually put before the US Supreme Court and on 29 June 2026, the US Supreme Court delivered its verdict.

The Supreme Court held that the previous ruling which provided commissioners with protection from US Presidents was unconstitutional as it limited the President's ability to exercise their executive powers.

How does this impact the EU-US Data Protection Framework (DPF)?

The EU-US DPF serves as the latest "adequacy decision" for transfers of personal data to the United States. A key element of the DPF is independent oversight and enforcement mechanisms to ensure the personal data of EU data subjects receives an equivalent level of protection in the US. The US established an independent judicial review body known as the Data Protection Court (DPRC) to fulfil this role. However, in light of Trump v. Slaughter, there are questions about whether judges in the DPRC can be fully independent if they can be removed at will.

What happens now?

There is no immediate change to the DPF, and organisations can continue to transfer personal data to third parties certified under the DPF to the US. However, activists have already indicated that they will challenge the adequacy decision and have called on the European Commission to repeal the DPF. Any legal challenge brought before the European Courts is likely to take years to reach its conclusion.

The Supreme Court ruling could have an impact on organisations who rely on Standard Contractual Clauses (SCCs) to transfer personal data. In order to rely on SCCs, you must conduct a Data Transfer Impact Assessment (DTIA) to ensure that data subject rights are respected in the destination country. If a DTIA has relied on the DPRC or the independence of the judiciary as evidence that the laws in the US can safeguard data subjects, you may need to revisit the DTIA to determine whether the transfer can proceed or if additional supplementary measures may be required.

Key action: The DPF remains as a valid transfer mechanism for now. Organisations relying on SCCs to transfer personal data should review any existing DTIAs and consider whether any updates or additional supplementary measures are required in light of this ruling.

GDPR Certification as a transfer mechanism

On 16 April, the European Data Protection Board released its opinion approving the Europrivacy Certification as a transfer mechanism under Article 46 GDPR.

What is Europrivacy?

Europrivacy is the first European Data Protection Seal approved under Article 42 GDPR. The Europrivacy certification allows organisations to demonstrate that a specific processing activity complies with the GDPR. In order to achieve certification, the organisation must undergo an assessment by an approved certifying body.

What did the EDPB approve?

When Europrivacy was first approved, it was limited to processing taking place within the EU. An updated set of certification criteria was submitted to the EDPB to extend the scope of certification to cover the international transfer of personal data under Article 42 and Article 46 GDPR. The EDPB recognised the additional criteria as offering the additional safeguards necessary for it to be used as a transfer mechanism.

How will this work in practice?

Certification as a transfer mechanism will operate similarly to how organisations transfer personal data with DTIAs and SCCs. In order to rely on certification, the exporter must have in place binding commitments from the importer (through SCCs). The exporter will still need to demonstrate that the data will receive an equivalent level of protection in the destination country by completing a DTIA, however the Europrivacy certification will streamline the assessment as the Europrivacy criteria will help address some of the risks with transfers to non-adequate countries.

Key action: Monitor the roll out of GDPR certification.

Recent fines

Midlands regional hospital Tullamore

The DPC has fined the HSE €300,000 for multiple violations of the GDPR in relation to a personal data breach. In 2018, the HSE discovered that there had been a ransomware attack on the laboratory information system in the Midlands Regional Hospital. The ransomware had given the attackers access to the results of patients' tests and subsequently encrypted those results. The HSE estimated that 84,000 data subjects were impacted by the breach.

Key facts

During the course of its investigation, the DPC found that the HSE had violated:

- Article 5(1)(f) GDPR by failing to ensure security of the patients' personal data.
- Article 28 GDPR by failing to ensure that agreements with third parties who processed personal data on the HSE's behalf included sufficient safeguards to ensure that processing was compliant.
- Article 30 GDPR by failing to have a complete Record of Processing Activity at the time of the breach.
- Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to safeguard patient data.
- Article 34 GDPR by failing to provide the impacted data subjects with all information required by that Article.

Finding

In addition to the fine of €300,000, the HSE was ordered to implement specific policies and procedures to ensure appropriate security of processing of personal data.

Key action: Ensure that technical and organisational controls are in place to safeguard personal data are appropriate to the risk presented by the nature of the processing, or the nature of the data being processed. Ensure that where you engage any third-party processors to process data on your behalf that those processors have appropriate controls to safeguard personal data.

Permanent TSB

The DPC has fined Permanent TSB (PTSB) €277,500 for multiple violations of the GDPR in relation to a series of personal data breaches. In 2022, PTSB notified the DPC that three malicious actors had called PTSB's customer service and impersonated customers in order to access those customers' accounts after the PTSB had failed to follow appropriate security protocols. Once the malicious actors had access to the victims' account they were able to obtain additional information about the victims and change their account details.

Key facts

During the course of its investigation, the DPC found that PTSB had violated:

- Article 5(1)(f) GDPR by failing to ensure appropriate security of customer accounts.
- Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure appropriate security while processing personal data through its customer service centre.
- Article 33(1) by failing to notify the DPC of the data breach within 72 hours of becoming aware of the breach.

Finding

The DPC fined PTSB €250,000 for failing to implement appropriate technical and organisational measures to keep data secure and a further €27,500 for failing to report the breach within the regulatory timeframe.

Key action: Ensure that technical and organisational controls are in place to safeguard personal data are appropriate to the risk presented by the nature of the processing, or the nature of the data being processed. Ensure your breach reporting procedure allows your organisation to meet its reporting obligation within 72 hours.

Social media-based marketing – Datatilsynet fine

We have seen continued regulatory scrutiny on the sharing of personal data with third parties for targeted advertising. The Norwegian data protection authority, Datatilsynet, recently issued a €1.7 million fine for sharing the personal data of 6 million loyalty programme members for targeted advertising.

Datatilsynet's investigation found that Elkjøp's loyalty programme consent statement was non-compliant as it bundled several marketing activities and did not allow for granular consent. Elkjøp also failed to provide sufficient information on sharing of personal data with social media platforms in their privacy notice.

During the investigation, Elkjøp argued that its sharing of personal data for customer match tools was actually based on Article 6(1)(f) legitimate interests. This defence was dismissed by Datatilsynet on the basis that the data was clearly collected on the basis of consent, and allowing processing on the basis of legitimate interests would undermine this consent.

This fine and the CNIL fine we covered earlier this year, demonstrate that transparency is an area of focus for regulators. Both of these investigations were cross-border cases which means that other data protection authorities agree with the findings and therefore would likely issue similar decisions if investigating organisations in their own countries.

These cases also highlight the importance of conducting a Data Protection Impact Assessment prior to commencing any new processing activities. As part of the DPIA process you will identify the most appropriate lawful basis for the processing and identify any actions necessary to ensure that lawful basis is valid.

Key action: Ensure your lawful basis is clear prior to processing personal data. You should not switch to legitimate interests to try to salvage a processing activity for which you have no valid lawful basis. Consider conducting a DPIA prior to introducing a new processing activity to identify the correct lawful basis and take steps to ensure the lawful basis is valid.

Developments in AI - update on Digital Omnibus Package

In 2025, the European Commission announced its intention to simplify the European Union's digital laws through the Digital Omnibus. The European Commission recently published its latest proposed amendments, and the main changes are as follows:

- Postpone the date of application of high-risk AI rules from 2 August 2026 to 2 December 2027 for Annex III systems and 2 August 2028 for Annex I systems.
- Providers of generative AI systems already on the market before 2 August 2026 will be given an additional six months to comply with their transparency obligations with AI-generated content.
- Remove the mandatory obligation for deployers and providers of AI systems to ensure AI literacy amongst staff. The European Commission and Member States will be responsible for promoting AI literacy initiatives instead.
- Providers and deployers of AI systems may process special categories of personal data to ensure bias detection and correction, provided appropriate safeguards are in place.
- Providers of AI systems will no longer have to register their AI systems with the EU database, provided the AI systems are not considered high-risk.
- The special considerations given to penalties for Small-Medium Enterprises (SMEs) has been expanded to include Small Mid-Cap (SMC) enterprises.

Key action: Monitor updates as negotiations continue around the Digital Omnibus.

Contacts

Liam McKenna
Partner
lmckenna@mazars.ie

David O'Sullivan
Director
DOSullivan@mazars.ie

Lisa Clarke
Senior Manager
Lisa.clarke@mazars.ie

Forvis Mazars Group SC is an independent member of Forvis Mazars Global, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 40,000+ professionals across the globe to assist clients of all sizes at every stage in their development.

forvismazars.com/ie