Data protection newsletter
Issue 22

This issue covers significant updates in EU, UK and international data protection law, including rulings on the EU–US Data Privacy Framework and the EU Data Act. It highlights key changes in the UK Data (Use and Access) Act and forthcoming GDPR amendments for small and mid-cap businesses. Recent enforcement actions and fines are also detailed, providing actionable insights for organisations. Stay informed on compliance, data transfers and regulatory trends to help protect your business.

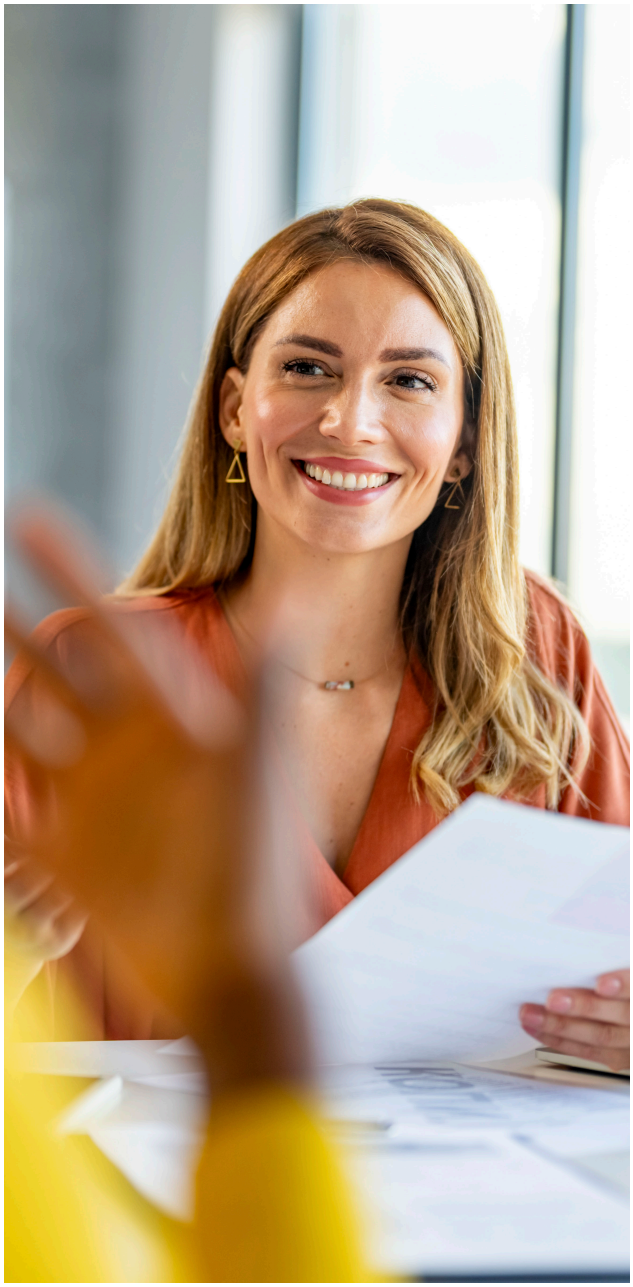
The EU-US Data Privacy Framework

On 3 September, the European General Court dismissed a case brought by a French member of parliament, who had filed a legal action in September 2023 to annul the EU–US Data Privacy Framework (DPF). The case argued that the Data Protection Review Court (DPRC) lacked independence and impartiality, and that the bulk collection of data by US intelligence agencies violated several articles of the Charter of Fundamental Rights of the EU.

The Court found that the DPRC includes sufficient safeguards and meets the "essentially equivalent" standard of independence required under EU law. It stated that US laws do not allow bulk collection of personal data within the US, instead permitting only targeted collection. The Court also noted that there is nothing in Schrems II to suggest that bulk collection must be subject to prior authorisation by an independent judicial authority. Rather, it must be subject to ex post judicial oversight, which the DPRC provides.

This ruling upholds the validity of the EU–US DPF, providing certainty for over 3,000 US companies relying on the framework for data transfers. The European Commission must continue to monitor the DPF's application and can suspend or amend it if US laws change. For now, companies can continue transferring personal data to the US under the DPF, although the ruling may still be appealed to a higher court.

Key action: The DPF is likely to face further challenges. Organisations should consider using Standard Contractual Clauses (SCCs) and Data Transfer Impact Assessments (DTIAs) as alternative mechanisms for data transfers.



The Data Act now in force

The EU Data Act became applicable on 12 September. This new EU law sets out how data, especially from connected devices, is accessed, shared and used fairly across the EU. Its main aims are to:

- Make data more accessible.
- Promote data-driven innovation and competition.
- Give users more control over the data generated by their connected products (smart devices).
- Make it easier for users to switch between data-related services.
- Ensure fairness in how data is shared and used.

Enable public sector access to data during emergencies. The Data Act covers both personal and non-personal data, with obligations primarily relating to "product data", data generated from the use of a connected product and related service data.

It applies to a wide range of participants, including:

- Manufacturers of connected products, like smart appliances and connected cars (telematics).
- Providers of related digital services, e.g. apps or platforms that work with those products.
- Users of connected products or services, both individuals and businesses.
- Data holders, anyone who has the right or obligations to use and share data.
- Data recipients, businesses receiving data from data holders.
- Cloud and data processing service providers, companies offering services like cloud storage and computing.

What does it mean?

Users have the right to access data generated by their connected products or services, request to share data with third parties and also have the right to switch cloud/ data services easily without unfair fees.

Data holders must make data available to users and third parties as requested fairly and transparently, protect personal data and trade secrets and can charge a reasonable fee for sharing data, but not for personal data or in emergencies.

Key action: Consider your business and if you need to comply with the Data Act.

The UK Data (Use and Access) Act 2025

The UK has introduced the Data (Use and Access) Act ("the Act"), which amends the UK GDPR rather than replacing it. The adequacy decision between the European Union and the United Kingdom was due to expire on the 27 June 2025. Due the UK government introducing the new Act, the European Data Protection Board (EDPB) concluded that there should be an extension for six-months and will review once the law is in place.

Main changes being introduced:

- **Lawful basis:** New legal basis in article 6 of the UK GDPR with providing an option to outline a 'recognised legitimate interests', such as fraud prevention and network security. These interests do not require a balancing test to be done.
- **Scientific research:** The Act redefines scientific research provisions. Commercial research, privately funded research and any reasonably scientific research fall within the scientific research exemption under Article 89(2) of the UK GDPR. The Act allows for broader consent for general research purposes to be obtained.
- **Subject access requests:** The Act confirms that organisations must provide personal data after it has conducted a "reasonable and proportionate" search. The Act now also allows organisations to "stop the clock" of the response timeframe while awaiting further information to help it identify the processing covered by the request.
- **International transfers:** The act in schedule 7 repeals article 44 and 45 of the GDPR and replaces it with new provisions for governing international transfers, there is change of terminology from adequacy decisions to "adequacy regulations" and introduces a new test for assessing a third countries data protection safeguards are not materially lower than the UK.
- **Regulatory enforcement:** The enforcement of the Privacy and Electronic Communications Regulations is now treated the same as the GDPR, where organisations can now be fined £17.5 million or 4% global turnover whichever is greater.
- **Cookies and other similar tracking technologies:** The Act outlines that cookies used for improving services, websites and security purposes will be exempt from the consent requirement.

Key action: For organisations based in the UK, review current practices and procedures and see if they align with areas such as recognised legitimate interests, cookie consent, Subject Access Requests and make adjustments as necessary. If you are conducting marketing via email that falls under the E-privacy regulations be aware that the maximum fines applicable have increased significantly to GDPR levels.

GDPR Omnibus

On 6 May, the European Commission adopted a Single Market Simplification proposal which included amendments to the GDPR as part of the Omnibus IV Simplification Package targeting small mid-cap enterprises (SMCs). A key focus is extending existing GDPR exemptions, currently available to small and medium enterprises (SMEs) to a wider group of businesses that have grown beyond the SME threshold but still face disproportionate compliance burdens.

On 8 May, the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) published a letter expressing their preliminary support for the simplification of obligations related to records of processing, noting that this would not impact the obligations of controllers and processors to comply with other GDPR obligations.

Key changes

- **Small-mid cap enterprises:** The proposal aims to define small mid-cap enterprises as organisations with fewer than 750 employees, a total balance sheet not exceeding €129 million and an annual turnover not exceeding €150 million.
- **Records of processing activity:** Currently under article 30 of the GDPR, the requirement to maintain records of processing does not apply where an organisation has fewer than 250 employees, unless the data processing is "likely to result in a risk to the rights and freedoms of data subjects". It is now proposed to extend the derogation on the obligation to maintain records of processing to SMCs as long as the processing does not result in a high risk to the rights and freedoms of data subjects.

- The Commission is also proposing modifying article 30(5) GDPR to provide that the derogation on maintaining records of processing would not apply if the processing is 'likely to result in a high risk to the rights and freedoms of natural persons' compared to the current provision that refers to processing likely to result in a 'risk'. The EDPB and EDPS support this proposal concerning 'likely high risk' processing as they note that even very small companies can still engage in high-risk processing and its therefore important to retain a risk-based approach.
- **Codes of Conduct:** GDPR article 40 encourages associations and other bodies representing categories of controllers or processors to draw up codes of conduct, taking account of the specific features or the various processing sectors and the specific needs of micro, small and medium sized organisations. This scope should be extended to SMCs so that their specific needs are also taken into account when codes are drawn up.
- **Certification:** Article 42 encourages the establishment of data protection certification mechanisms, seals and marks by certification bodies or competent bodies, considering the specific needs of SMEs. The proposal extends this provision to include the specific needs of SMCs.

Key action: Consider your business and if you need to comply with the Data Act.

Recent fines

City of Dublin Education and Training Board (CDETB)

The DPC has fined the CDETB €125,000 for multiple GDPR violations in relation to a data breach. In November 2018, the CDETB discovered that its webserver was retaining personal data of student grant applicants and had been compromised by malware. Approximately 13,000 individuals were affected, with data including names, birth dates, PPS numbers, contact and identification details, and special category data such as racial/ethnic origin and health information.

Key facts

Breach notification

- The DPC found that CDETB violated article 33(1) GDPR by failing to notify the DPC within the 72-hour window.
- The DPC also found that CDETB breached article 34(1) and 34(4) by not notifying affected individuals affected by the breach and also for failing to comply with the DPC's request to notify the individuals.

Technical and organisational measures

- The DPC found there were multiple violations of Article 5 and 32, in regard to a failure to implement appropriate technical and organisational measures.

Findings

- In addition to the fine, the DPC imposed the following penalties on CDETB. A formal reprimand and an order to bring data processing activities into compliance with GDPR security requirements.

Key action: Review internal breach management procedures and ensure they are robust and include notification as necessary to the DPC and data subjects.

TikTok

The DPC has fined TikTok €530 million for violations of the GDPR for unlawful transfers of EEA user personal data to China, this was through remote access by Chinese staff. This announcement follows on from an inquiry launched into TikTok in September 2021 on the transfers of EEA personal data to the China and the organisation's transparency in informing users of the transfers.

Key facts

Data transfers

- During the inquiry, TikTok provided the DPC with an assessment of the Chinese legal framework, highlighting that Chinese laws such as the National Intelligence law and Cybersecurity Law don't offer protection equivalent to EU Law, but claimed their transfers were not affected by the laws in question.
- The DPC found that TikTok violated Article 46(1) GDPR by failing to prove their measures and Standard Contractual Clauses provided essentially equivalent protection to EU Law.
- The DPC also found that TikTok's inadequate assessment of Chinese law impacted their ability to choose proper safeguards and supplementary measures.

Transparency

- TikTok's 2021 EEA privacy policy violated Article 13 GDPR by not disclosing remote access to personal data in Singapore and the US by personnel in China.
- In 2022, TikTok updated the policy to include all third countries receiving EEA data and explained the transfer process, which the DPC found compliant.

Findings

- In addition to a €530 million fine, TikTok have been ordered to bring their processing into compliance within six months, the DPC also set out an order to suspend their transfers to China if this wasn't complied with.

Key action: Ensure to provide transparency to users of the transfer of their personal data to countries outside the EEA/EU and the appropriate safeguards being relied on.

Department of Social Protection ("DSP")

The DPC has been fined €550,000, after concluding its inquiry, launched in July 2021 into the DSP's use of biometric data as part of the SAFE 2 registration process for issuing Public Services Cards ("PSC"). SAFE 2 is an identity verification process for accessing services, including social welfare payments. It requires individuals to submit to facial image capture, which is then used to create a biometric template. By 2021, the DSP had collected biometric data for approximately 70% of Ireland's population.

Key facts

Inadequate legal basis

- The DPC found that there was no lawful basis for the collection of biometric data in connection with SAFE 2 registrations.
- The absence of supporting legislation creates a risk of arbitrary interference with individuals' privacy rights.
- The DPC emphasised that public policy goals such as the prevention of fraud do not override the need for lawful processing.

DPIA issues

- The DPC found that the DPIA did not sufficiently address the risks associated with the scale and sensitivity of biometric data.
- The DSP were unable to prove what safeguards were in place to mitigate risks to individual rights.

Findings

- The DPC also ordered them to cease processing of its biometric data within 9 months, if they are unable to identify a valid lawful basis.

Key action: DPIAs need to adequately and effectively address risks associated with the processing activity.

Contacts

Liam McKenna
Partner
lmckenna@mazars.ie

David O'Sullivan
Director
DOSullivan@mazars.ie

Lisa Clarke
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