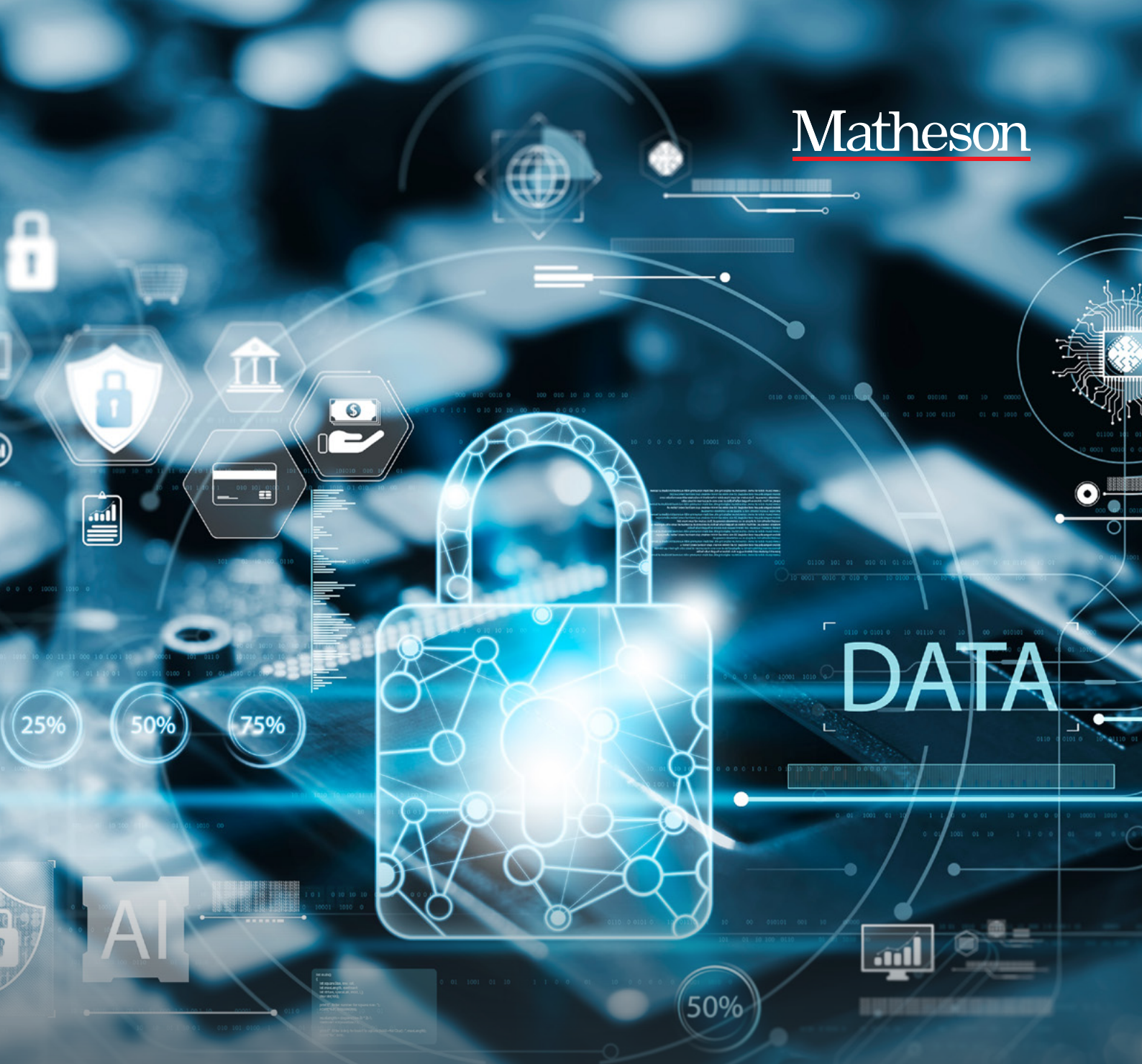

Matheson

World Data Protection Day 2026

Introduction

Over the past year, we have seen the Irish Data Protection Commission ("**DPC**") being active on many fronts. Whilst the DPC's regulation of AI model training and statutory inquiries launched in this area have continued to attract a lot of public interest, we have also seen the DPC impose heavy fines for a range of GDPR infringements. In particular, fines for breach of the core GDPR principles and related obligations, such as the fair, transparent and lawful processing and security principles, and the data transfer rules, continue to dominate the headlines.

The CJEU has also continued to provide guidance on a number of important GDPR concepts and obligations. Some of these CJEU decisions also demonstrate the challenges that companies are increasingly facing in light of the EU's evolving Digital Rulebook, and the interlapping obligations under various legislation.

Following publication of the Draghi and Letta reports in 2024, and demands for greater competition and simplification of the EU's Digital Rulebook, the European Commission published the draft Digital Omnibus Regulations on 19 November 2025. The draft Regulations aim to simplify and consolidate various EU digital laws concerning data, AI, cybersecurity and online platforms. Changes to the GDPR, the e-Privacy Directive, the AI Act, and the Data Act, amongst others are proposed. In particular, targeted amendments to the GDPR have been proposed, with the stated goal being to "*harmonise, clarify and simplify GDPR provisions*" without affecting its core principles.

The proposals include, for example, a clearer definition of what constitutes "personal data" under Article 4(1) GDPR; further clarity on when a data subject access request ("**DSAR**") can be refused or a fee charged on the basis that it is "excessive" under Article 12(5) GDPR; and relaxations to the current personal data breach notification obligations.

The response to the proposals has been mixed. Some privacy advocates argue that the proposals, which have been presented as "technical streamlining", could effectively involve the GDPR being "*reopened and hollowed out*". Others regard the proposals as not going far enough. The proposals are expected to face intense lobbying and debate regarding the balance between simplification of the EU's Digital Rulebook and the protection of individuals' fundamental data protection rights and freedoms (further Matheson commentary here).

In this briefing note, our Technology and Innovation Group discuss some of the most important data protection-related developments from 2025.

DPC fines and regulatory activity

- **The DPC's Annual Report for 2024**, published on 19 June 2025, provides an overview of all key regulatory activity undertaken by the DPC during 2024. In line with previous years, the top three categories of complaints to the DPC concerned: (i) the right of access (34%); (ii) fair processing (17%); and (iii) the right to erasure (14%). Matheson commentary on the Annual Report and Case Studies is available here.

- **€530m fine imposed on TikTok for breach of transparency and data transfer rules** - Following the DPC's Inquiry into TikTok's transfers of EEA user data to China, the DPC found that TikTok had failed to comply with the data transfer rules under Article 46 GDPR, and the transparency obligations under Article 13 GDPR. In particular, the DPC found that TikTok failed to provide sufficient information to users in its privacy notice regarding its data transfers, including the names of the non-EEA countries it was transferring data to, and the nature of the privacy operations constituting the transfer (namely remote access to personal data stored in Singapore and the US by personnel based in China).
- **€550,000 fine imposed on the Department of Social Protection for processing special category data without a lawful basis and in breach of the transparency obligations** – The DPC imposed this fine for collecting biometric data without a valid lawful basis under Articles 5(1)a, 6 and 9 GDPR in respect of the processing of biometric facial templates, and associated use of facial matching technologies as part of the registration process for the Public Services Card. The Department also failed to comply with its transparency obligations to data subjects under Article 13 GDPR, and failed to include the required details in its Data Protection Impact Assessment ("**DPA**"), thereby infringing Article 35 GDPR.
- **€125,00 fine imposed on the City of Dublin Education and Training Board ("CDETB") for infringing the security and personal data breach notification obligations** - This fine was imposed following the conclusion of the DPC's Inquiry into the CDETB for failure to implement appropriate security measures and report a personal data breach to the DPC and affected data subjects without undue delay. The CDETB also failed to communicate the breach to affected data subjects when directed to do so by the DPC, in breach of Article 34(4) GDPR.

EU DPA regulatory activity

Data Protection Authorities ("**DPAs**") across the EU have been active throughout 2025. Below we list some of the most significant fines issued over the past year. These fines align with the enforcement trends we have seen from the DPC, including sanctions for non-compliance with the core GDPR principles and related obligations, along with breach of the data transfer rules.

- **Transfer of personal data** – A telecommunications operator was fined €4.5 millon by the Croatian DPA for non-compliance with the GDPR, including for unlawful transferring of personal data to third countries. The telecommunications operator performed the transfer without valid transfer safeguards in place (including a failure to carry out a Transfer Impact Assessment) and failed to provide sufficient transparency information to data subjects in respect of the data transfer. In addition, it had no legal basis for processing copies of employees' identity cards and certificates of no criminal proceedings (read more here).
- **Third party processing of personal data and security deficiencies** – Poland's DPA fined a fast-food outlet €4 million in respect of an employee data breach caused by a third-party processor. The third-party processor, who had been engaged to manage work schedules, accidentally exposed the employee data (names, IDs, passport numbers, work details) due to a misconfigured server. The processor had also engaged sub-processors without proper agreements. The fast-food outlet, as controller, was fined for infringing GDPR rules on controller accountability, processor oversight and due diligence, data minimization, and failure to include its DPO in critical compliance processes. The decision serves as a reminder that outsourcing data processing does not remove controller responsibility (read more here).

- **Third party processing of personal data and security deficiencies** – A German DPA fined a telecommunications operator €45m for failing to carry out appropriate due diligence on third party processors in line with Article 28 GDPR, and for security flaws in in its online portal which enabled unauthorised access to customer data. The DPA noted that many companies had an investment backlog in modernising and consolidating IT systems (read more here).
- **Balancing AI innovation and data protection compliance** – The Italian DPA fined Luka Inc. €5 million for infringements of the GDPR in relation to its Replika service, a chatbot-based generative AI system. The DPA found that the controller did not identify a legal basis for the data processing operations carried out through Replika. In addition, the privacy policy was inadequate. Furthermore, despite declaring minors were excluded as potential users, the company had not implemented any age verification mechanism (read more here).
- **Lawful, fair and transparent processing** – The Dutch DPA fined a credit reference agency €2.7 million for violations of the GDPR. The agency provided credit score ratings on individuals at the request of its customers, including landlords, telecommunications companies and retailers. The score indicated a person's ability to pay their bills and whether there was a risk of default. The agency's customers used the credit score to decide whether and how individuals were eligible to purchase a product. The DPA launched an investigation after receipt of complaints from individuals who were required to pay a high deposit when switching energy suppliers or were denied credit by service providers. The DPA found various breaches of the lawful, fair and transparent processing principle and related-obligations (read more here).

GDPR-related CJEU decisions

- **Scope of definition of personal data** – In EDPS v SRB (Case C-413/23 P), the CJEU provided some much-needed clarity regarding the scope of the definition of "personal data" under the GDPR. The CJEU confirmed that pseudonymised data may not constitute personal data in all cases. Instead it may be "personal data" for the initial controller, but not for a third party recipient if that third party does not have "means that are reasonably likely" to reverse the pseudonymisation and re-identify the relevant data subjects.
- **Application of the "soft opt-in" rule for electronic direct marketing purposes** – The CJEU decision in Inteligo Media SA v ANSPDCP (Case C-654/23), clarifies the scope of the "soft opt-in" rule in respect of electronic direct marketing to customers. The default rule under the ePrivacy Directive (2002/58/EC) is that an organisation needs to obtain an individual's prior consent before sending them direct marketing emails. An exception (i.e. a "soft opt-in") applies in circumstances where an organisation obtains an individual's email address "in the context of the sale of a product or a service". The CJEU confirmed that that the term "sale" does not necessarily require direct remuneration for a good or a service, and that indirect remuneration may suffice (Matheson commentary here).
- **GDPR liability of online marketplaces for user-published advertisements** – The CJEU held in X v Russmedia and Inform Media Press (Case C-492/23) that an operator of an online marketplace may be classified as a "joint controller" with a user of that platform, in respect of any user-posted advertisements containing personal data. This will occur in circumstances where the operator exercises "decisive influence" over such user-posted advertisements. The CJEU further confirmed that the liability exemptions under the e-Commerce Directive (or its successor, the Digital Services Act), do not override the GDPR obligations of the operator of an online marketplace (Matheson commentary here).
- **Calculating GDPR fines for corporate groups** – The CJEU in IVLA A/S (Case C-383/23) confirmed that for the purposes of calculating the maximum administrative fine applicable under the GDPR for a subsidiary's non-compliance, the total turnover of the parent company should be considered. This is due to the fact that the definition of an "undertaking" under the GDPR includes the wider group that the subsidiary is part of. The decision underscores the principle that financial penalties should reflect the economic reality of corporate groups, reinforcing the broad liability of parent companies under the GDPR.

- **Balancing transparency on automated decision-making and trade secrets** – The CJEU ruled in Dun & Bradstreet Austria GmbH (Case C-203/22) that Article 15(1)(h) GDPR requires data subjects to receive "meaningful information" about any automated decision-making, including profiling, to ensure transparency and enable challenges to such decisions. The CJEU ruling confirms that it is not sufficient for a controller to merely communicate the algorithm used to make the decision, as this would not constitute "a sufficiently concise and intelligible explanation". Instead, a controller must describe the decision-making procedure in a way that allows data subjects to understand which of their personal data have been used and how. It is also clear that trade secrets do not justify opacity. If a controller believes that certain information forms part of a trade secret, they must provide the allegedly protected information to the competent court or supervisory authority, and it is for that body to determine the scope of information to be provided, having regard to the rights and interests at issue.
- **Manifestly excessive or repetitive complaints to supervisory bodies** - In Österreichische Datenschutzbehörde (Case C-416/23), the CJEU held that DPAs cannot refuse to act on a complaint submitted by a data subject by characterising it as "excessive" under Article 57(4) GDPR, simply because the data subject has filed several complaints with the same DPA. Rather an abusive intention on the part of the requestor must be established. This decision is also relevant to controllers who receive voluminous or repeated requests from data subjects. Article 12(5) GDPR contains similar wording to Article 57(4) GDPR, enabling controllers to refuse manifestly excessive or repetitive requests from data subjects (Matheson commentary here).
- **Consideration of the data minimisation and lawful processing principles** – In Mousse v CNIL (Case C-394-23), the CJEU held that a title (i.e. Mr or Mrs) constitutes "personal data" under the GDPR, as it reflects the gender identity of the data subject. The CJEU found that a controller must establish an appropriate legal basis for processing such personal data, such as necessary for the performance of a contract or the legitimate interests pursued by the controller or by a third party. In this case, it was found that requiring customers of a rail transport company to provide their title when purchasing tickets online constituted a breach of the data minimisation and lawfulness principles.

Compensation claims for non-material damages

- In Quirin Privatbank (Case C-655/23), the CJEU ruled that the term "non-material damage" within the meaning of Article 82 GDPR may include "negative feelings" experienced by the data subject, such as fear or annoyance, which are caused by the loss of control over personal data. However, the Court ruled that the mere assertion of negative feelings is insufficient for compensation. The national courts must assess evidence of such feelings, and be satisfied that they arose following an infringement of the GDPR.
- The case of Bindl v European EU Commission (Case T-354/22) was the first time that an EU court awarded compensation to an individual for non-material damages in respect of an infringement of EU data transfer rules. Whilst the issues in scope of the decision relate to Regulation 2018/1725/EU (the equivalent of the GDPR for personal data processing carried out by EU institutions), the findings will be of relevance to organisations that are subject to the GDPR, which contains similar provisions (Matheson commentary here).
- In OC v EU Commission (Case T-384/20), the EU General Court granted the plaintiff an award of €50,000 in non-material damages for harm to her reputation and health caused by a press release from the European Anti-Fraud Office ("**OLAF**") that conveyed false information about her. Similar to the Bindl case, the decision concerned Regulation 2018/1725/EU. Interestingly, the data subject was not named in the relevant press release, but it was determined that it was "reasonably likely" that she was identifiable from the information contained in the press release.
- In Dillon v Irish Life Assurance PLC [2025] IESC 37, the Irish Supreme Court held that non-material loss claims under the GDPR, in respect of distress, upset, anxiety and inconvenience, are not in the nature of personal injuries, and therefore do not require authorisation from the Injuries Resolution Board prior to commencing proceedings. This is an important decision as it removes what was previously a procedural hurdle for claimants, making it more straight-forward to now bring such claims (Matheson commentary here).

- In Walsh v Irish Prison Service [2025] IECC 8, the Irish Circuit Court delivered another significant decision concerning compensation for non-material damage under the GDPR. The Court applied the guidelines set out in Kaminski v Ballymaguire Foods [2023] IECC 5 (discussed previously here) and dismissed the plaintiff's claim on the basis that the plaintiff had suffered no more than "mere upset". In addition, the Court found there was no evidence of a causal link between the GDPR infringement and the alleged damage suffered. The decision reaffirms the now well-established principle that mere GDPR infringements will not give rise to compensation in themselves, and that "mere upset" alone is not compensable (Matheson commentary here).

Irish litigation

- **High Court declines to judicially review DPC refusal to investigate** – In McShane v Data Protection Commission and Health Service Executive ("**HSE**") [2025] IEHC 191, the Irish High Court rejected a judicial review application in which a HSE employee sought to challenge the DPC's decision not to investigate a personal data breach complaint. The employee used a work mobile phone for personal use and alleged that, as a result of the cybersecurity breach at the HSE, he suffered a personal data breach and personal loss. In particular, he attributed the cybersecurity breach as leading to his personal email account and cryptocurrency account being hacked, and €1,400 of cryptocurrency stolen.

  The DPC had declined to investigate the complaint on the basis that the HSE was not the "data controller" of the relevant personal data, because using the work phone for personal purposes was contrary to the HSE's acceptable use policy. The High Court rejected the judicial review application on the basis that the DPC's decision was not irrational and within its lawful authority. The decision serves as an important reminder for employers to ensure they have appropriate acceptable use policies in place in respect of their use of work devices.

EDPB guidance and coordinated enforcement actions

- **Interplay between the Digital Markets Act ("DMA") and the GDPR** – The EDPB and the European Commission issued joint guidelines aimed to ensure that the DMA and the GDPR are interpreted and applied in a compatible manner. Whilst the GDPR aims to protect individuals with regard to the processing of their personal data, the DMA aims to tackle unfair practices, and their potential harmful effects for business users. The guidelines provide clarity on key issues such as user consent (Article 5(2) DMA), third-party software applications and stores as controllers (Article 6(4) DMA), data portability (Article 6(9) DMA and Article 20 GDPR), right of data access (Article 6(10) DMA), contestability in the online search engine market (Article 6(11) DMA) and interoperability to alternative service providers (Article 7 DMA).
- **Guidelines 3/2025 on the interplay between the Digital Services Act ("DSA") and the GDPR** – The EDPB issued guidelines to contribute to the consistent interpretation and application of the DSA and the GDPR where there is overlap regarding the processing of personal data. The guidelines focus on efforts to detect, identify, and address illegal content (Article 7 DSA), complaint mechanisms (Article 20 DSA), account suspension (Article 23 DSA), deceptive design patterns (Article 25 DSA), transparency in advertising (Article 26 DSA) and management of systematic risk (Articles 34 and 35 DSA).
- **Guidelines 02/2024 on Article 48 GDPR** – These guidelines provide practical recommendations for controllers and processors in the EU that may receive requests from third country authorities to disclose or transfer personal data. They emphasise that the objective of Article 48 GDPR is to clarify that judgments or decisions from third country authorities cannot automatically and directly be recognised or enforced in an EU Member State. Rather, as a general rule, recognition and enforceability of foreign judgements and decisions is ensured by applicable international agreements.
- **EDPB Coordinated Enforcement Action for 2026: Transparency and information under the GDPR** – For 2026, the EDPB has confirmed that it will be launching a coordinated enforcement action focused on compliance with the transparency and information obligations under Articles 12, 13 and 14 GDPR. As part of the coordinated action, the EDPB will work with participating DPAs at national level, to investigate organisations' compliance

with this obligation. The EDPB will publish a Report on its findings in due course. Accordingly, organisations should ensure that their privacy notices contain the granular information expected by the DPC following its decision in respect of WhatsApp in 2021. In particular, organisations should ensure that their privacy notices identify a clear link between what categories of personal data are processed, the purpose(s) of such processing, and the relevant legal basis relied on.

DSARs

- **When a DSAR constitutes an abuse of GDPR rights** – In case C-526/24, Advocate General Spunzar delivered a significant opinion on when a data subject access request may be deemed to be an abuse of one's data protection rights and "excessive" under Article 12(5) GDPR. The opinion indicates that the decisive factor in identifying abusive intent is the underlying purpose of the data subject's actions, such as deliberately creating a relationship with the controller for the purpose of exploiting their data protection rights, and causing the controller to refuse the DSAR (Matheson commentary here).
- **Mixed record personal data** – The DPC clarified its approach to a mixed record of personal data in its recent blog on the DPC's handling of Subject Access Requests. The DPC confirmed that in circumstances where a controller holds a mixed record of personal data (i.e. containing personal data relating to the requester and a third party), that Article 15(4) GDPR permits the controller to withhold this information if its disclosure could adversely affect the other third party(ies) concerned. For example, an identified risk of harm to a spouse/partner/child, arising from the potential disclosure of the information to the requesting individual, could justify the withholding of the information concerned.
- **EDPB Coordinated Enforcement Taskforce Report on the Right of Access** – The EDPB published their Coordinated Enforcement Taskforce Report ("**The Report**") on "*Implementation of the right of access by controllers*" in January 2025. The Report identified challenges organisations are facing regarding the right of access. These challenges include a lack of awareness about the scope of the right of access; excessive or inconsistent retention periods relating to access requests; lack of documented internal procedures; excessive interpretations of the limits to the right of access; excessive interpretation of the possibility to ask for specification of access requests; and provision of insufficiently detailed or tailored information to data subjects about how their data is processed. Read more here.

International Data Transfers

- **Challenge to EU-US Data Privacy Framework ("DPF")** – In Latombe v Commission (T-553/23), the EU General Court dismissed an action for annulment of the European Commission's adequacy decision for the DPF. The Court confirmed that the US guaranteed an adequate level of data protection at the time of the adequacy decision (namely 10 July 2023). This means that, for the time-being, organisations can continue to rely on the DPF in order to transfer personal data from the EU to those US organisations that have self-certified to the DPF. However, the transfer of data pursuant to the DPF in the longer-term remains subject to some uncertainty, as the applicant in this case has lodged an appeal with the CJEU against the Court's decision (see case number C-703/25P).

- **European Commission's renewal of UK adequacy decisions** – In December 2025, the European Commission renewed the two 2021 UK adequacy decisions. These adequacy decisions means that businesses can freely transfer personal data from the EU to the UK, without the need to implement any additional safeguards under Chapter V GDPR (such as the SCCs). The UK adequacy decisions remain valid until 27 December 2031, with the possibility of being further renewed.

The EU digital legislative landscape

- **Proposal for a Regulation on simplification measures for SMEs and SMCs** (2025/0130) – This Proposal, often referred to as part of the Omnibus IV package, was published by the European Commission on 21 May 2025. It forms part of the EU simplification measures. The proposal would modify the derogation in Article 30(5) GDPR by providing that the obligation to keep a record of data processing activities ("ROPA") would not apply to organisations employing less than 750 people, unless the processing is likely to result in a high risk to individuals' rights and freedoms. Currently, this derogation only applies to enterprises and organisations which have under 250 employees, except in certain cases. In addition, the proposal would introduce a definition of small and medium sized enterprises ("SMEs") and small mid-cap enterprises ("SMCs") in Article 4 GDPR, and extend the scope of Article 40(1) and 42(1) GDPR to the SMCs.
- **Draft Digital Omnibus Regulations** – In November 2025, the European Commission published two draft Digital Omnibus Regulations (Regulations 2025/0360/EU and 2025/0359/EU). The proposed reforms seek to simplify the EU's digital laws, cut compliance costs for companies, and boost the competitiveness of companies operating in Europe. Regulation 2025/0360/EU proposes amendments to the GDPR, as well as other legislation such as the ePrivacy Directive, the Data Act and NIS2. In addition, it proposes the repeal of the Platform to Business Regulation, as its objectives are now largely covered by the DMA and DSA. Meanwhile, Regulation 2025/0359/EU proposes amendments to the AI Act (Matheson commentary here).
- **Digital Operational Resilience Act ("DORA")** (Regulation 2022/2554/EU) – DORA entered into application on 17 January 2025. DORA creates consistent digital operational resilience rules for the EU financial sector. It focuses on five pillars: (i) information and communication technology ("**ICT**") risk management; (ii) ICT-related incident reporting; (iii) digital operational resilience testing; (iv) ICT third-party risk management (including the introduction of an oversight framework for critical ICT third-party service providers); and (v) information sharing. In essence, it aims to ensure that banks, insurance companies, investment firms, and other financial entities can withstand, respond to, and recover from ICT disruptions, such as cyberattacks or system failures.
- **Network and Information Security Directive ("NIS2")** (Directive 2022/2555/EU) – NIS2 has not yet been transposed into Irish law, but the Government is expected to adopt national implementing legislation in early 2026. NIS2 is focused on enhancing cybersecurity preparedness within specific sectors of the economy and the key players within them that are deemed either "essential" or "important" to the economy of the State.
- **Data Act** (Regulation 2023/2854/EU) – Most of the provisions of the Data Act came into application on 12 September 2025. Applicable to both personal and non-personal data, the Data Act imposes significant, cross-sectoral obligations on manufacturers of connected devices and providers of cloud/edge services, aiming to empower users (both businesses and consumers) and foster a more competitive digital market. It aims to advance digital transformation by establishing a framework for data sharing, facilitating data access and implementing obligations on data processing providers to assist users switching between data processing providers, and promoting interoperability.
- **AI Act** (Regulation 2024/1689/EU) – The AI Act came into force 1 August 2024, with phased implementation through August 2026. See Matheson's comprehensive Guide to the AI Act (here). There were two key application dates last year, namely 2 February 2025 (for the prohibited practices rules and AI literacy obligations) and 2 August 2025 (for general purpose AI rules). The next key deadline is 2 August 2026, when certain high-risk AI rules are due to come into force. The Digital Omnibus AI Regulation 2025/0359/EU, however, proposes delaying this deadline by up to 16 months, namely to 2 December 2027 for those high-risk AI systems in Article 6(2) and Annex II of the AI Act, and 2 August 2028 for those high-risk systems in Article 6(1) and Annex I of the AI Act.

- **Cyber Resilience Act ("CRA")** (Regulation 2024/2847/EU) – The CRA entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027 and the reporting obligations under the CRA will apply from 11 September 2026. The CRA complements the NIS2 Directive by introducing cybersecurity requirements for manufacturers of "products with digital elements", such as hardware and software products that are connected, whether directly or indirectly, to another device or network.
- **GDPR Procedural Regulation** (2025/2518/EU) – This Regulation entered into force on 1 January 2026 (20 days after publication on 12 December 2025) and applies from 2 April 2027. It proposes to strengthen co-operation among EU DPAs through a structured cooperation framework, enhanced information sharing, early consensus building, mutual assistance and joint operations, dispute resolution mechanisms, common electronic tools, simplified procedures and transparency.

Contact us

Matheson's Technology and Innovation Group combines deep expertise in data protection, AI regulation, cybersecurity, online safety, e-commerce, and commercial law to help businesses anticipate and adapt as the EU's digital legislative landscape continues to evolve. We stand ready to guide you through the challenges and opportunities ahead, ensuring compliance, mitigating risk, and unlocking innovation in a rapidly changing legal and regulatory environment.

Marie McGinley

Partner | Head of Technology and Innovation
t +353 1 232 3722
e marie.mcginley@matheson.com

Davinia Brennan

Partner
t +353 1 232 2700
e davinia.brennan@matheson.com

Sarah Jayne Hanna

Partner
t +353 1 232 2865
e sarahjayne.hanna@matheson.com