WILLIAM FRY

// Technology

2024 Data Protection Round-Up and Emerging Trends for 2025

January 2025

Data Protection Day 2025: "Look Back" & Trends

William Fry LLP is celebrating the Council of Europe's annual Data Protection Day. As we approach the 7-year mark of GDPR, Europe's data protection regulatory regime remains a headline staple, featuring twists and turns in many areas. In 2024, there was a renewed focus on data protection compliance because of: (i) the interplay between GDPR and emerging digital reforms legislation across the EU; and (ii) guidance and decisions from courts and data protection authorities continued to emerge and, in some cases, moved the goal posts of the application of certain data protection rules.

In this update, our Data Protection & Cybersecurity group explore the most significant data protection developments from the past year, and take stock of expected trends for 2025. Whilst data protection law comes to the fore for organisations in many ways, each should consider the following key areas with scrutiny:

1. **Increased Privacy Litigation**
2. **International Data Transfers**
3. **Protection of Children's Data Online**
4. **GDPR and the EU Digital Reforms Package**
5. **Data Protection and Artificial Intelligence**
6. **GDPR and Cybersecurity**

1. Increased Privacy Litigation

Throughout 2024, there was an increase in data protection and privacy litigation at both a national and EU level. This section covers some of the most notable decisions in 2024. As a general theme, we have seen both national courts and the Court of Justice of the European Union (**CJEU**) adopt a data subject centric approach in decisions and opinions.

NATIONAL

January

The Commencement of Courts and Civil (Miscellaneous Provisions) Act 2023

The commencement of the Courts and Civil (Miscellaneous Provisions) Act 2023 now provides jurisdiction to the District Courts to adjudicate on data protection actions. It also provides a guide to possible compensation recoverable in a data protection action in the District Court. The impact of this legislation is that the quantum of damages in privacy litigation will likely remain low.

Keane v Central Statistics Office [2024] IEHC 20

In the *Keane* decision, the High Court clarified the procedural steps in data breach cases where the applicant claimed to have suffered anxiety and distress. O'Donnell J held that the plaintiff was required by the Personal Injuries Assessment Board Act 2003 (**PIAB Act**) to make an application to PIAB for an assessment of her claims prior to commencing proceedings.

April

Dillon v Irish Life [2024] IEHC 203

In *Dillon*, the High Court considered whether the applicant's claim for damages due to alleged distress, upset, and inconvenience resulting from breaches of data subject rights constituted a 'civil action' requiring authorisation from PIAB under the PIAB Act. O'Donnell J, in revisiting his previous judgment of *Keane*, held that the proceedings brought by the plaintiff were a form of civil action within the meaning of the PIAB Act and as such required prior authorisation from PIAB.

July

McCabe v AA Ireland [2024] IECC 6

In *McCabe*, the Dublin Circuit Civil Court awarded the plaintiff €5,500 together with costs to the plaintiff as non-material damages for a GDPR infringement in circumstances where the plaintiff had not made a prior application to PIAB. This decision follows the earlier *Dillon* decision (above); a ruling by the Supreme Court on appeal in the latter may bring further clarity on how these cases can be reconciled.

EU

May 2023

Financial compensation for non-material damage sought in multiple decisions

Following delivery of judgment in *UI v Österreichische Post AG* (the "Austrian Post" case) in May 2023, in which the CJEU established the parameters of non-material damage claims under Article 82 of the GDPR for the first time, the EU courts have seen an increase in claims by individuals who have suffered non-material damage as a result of infringement of the GDPR. Read our insights on the Austrian Post case here.

September

- Case-768/21 held that data protection authorities are not always obliged to exercise their corrective powers, specifically to impose an administrative fine, where such an action is not *"necessary and proportionate to remedy the shortcoming found and to ensure that that regulation is fully enforced"*.
- Case C-383/23 considered that the meaning of 'undertaking', as defined in Articles 101 and 102 of TFEU, should be considered in calculating fines. The implication of the decision means that the total annual worldwide turnover of an undertaking of which the controller or processor forms part could be taken into account.

October

- In Case C-507/23, the CJEU held that making an apology can constitute sufficient compensation for non-material damage in certain circumstances and an infringement alone does not constitute damage requiring compensation.
- Case C-200/23 held that a "*loss of control*" for a limited period by a data subject may be sufficient to constitute non-material damage.
- Case C-21/23 held that products concerning health can be categorised as special category data.
- Case C-621/22 held that purely commercial interest can be a valid legitimate interest, which is a positive outcome for organisations.

2025 Trends

PIAB Authorisation needed prior to commencing a claim in the Irish courts?

In *Dillon*, the Supreme Court granted the plaintiff leave to appeal on the grounds of constituting an issue of 'general public importance'. If the decision is upheld, future plaintiffs must continue to seek PIAB authorisation prior to commencing a claim, again setting a clear recognition for similar claims regarding breach of privacy rights for data subjects in the context of non-material damage (claims relating to stress, humiliation or embarrassment). The case is scheduled for hearing in the Supreme Court on 30 January 2025.

Increased litigation on right to non-material damages

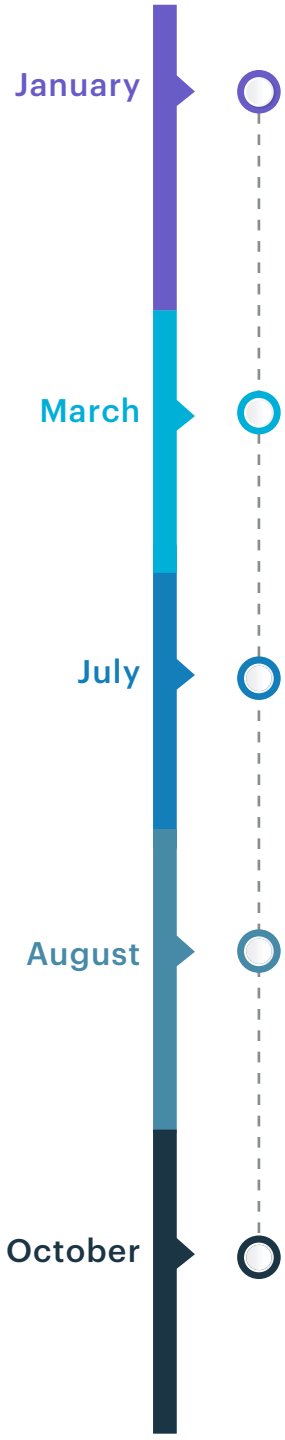
Following delivery of judgment in the *Austrian Post* case, both EU and national courts may continue to see an increase in claims by persons who have suffered non-material damage as a result of infringement of the GDPR and are seeking compensation from the controller or processor. Court decisions will continue to shape an appropriate compensation framework. In January 2025, Case T-354/22 (*Bindl v European Commission*) entitled the data subject to €400 in compensation resulting from the transfer of that data subject's personal data to a third country without an adequate safeguard in place in relation to the data transfer. Equally, we may witness an increased sentiment in decisions that *actual* damage must be suffered in order to give rise to compensation; and that a mere infringement of the GDPR is not, in itself, sufficient for compensation (as per Austrian Post).

Broader approach of regulators to Anonymisation

Back in 2023, in Case T-557/20 (*SRB vs SDPS*), the European General Court held that pseudonymised data will be considered anonymised data if the *holder* of such data has no means to (re-) identify the individuals about whom such data relates. The decision, which is currently under appeal to the CJEU, could arguably be a game-changer for organisations sharing data, as it marks a departure from the high bar of data anonymisation established in previous CJEU case law (in the *Breyer* decision). If upheld, the impact will mean that the GDPR will not apply to any personal data transferred where the recipient has no legal means to identify individuals from the data. Organisations will be watching closely as the appeal is expected to be heard by the end of January 2025.

2. International Data Transfers

2024 marked a period of steady activity in the sphere of international data transfers, visible in a high-profile administrative sanction imposed on Uber by the Dutch data protection authority; and key publications from the European Data Protection Board (**EDPB**) and Information Commissioner's Office (**ICO**). We also witnessed the continued negotiation and conclusion of adequacy decisions by the European Commission; and fines for companies deemed to be in breach of the GDPR in relation to international data transfers.



European Commission concluded review of 11 adequacy decisions

The European Commission concluded its review of 11 adequacy decisions which had been adopted under EU data protection legislation that preceded the GDPR. The Commission concluded that the adequacy decisions adopted for the 11 countries (including Guernsey, the Isle of Man, Jersey and Switzerland) continue to benefit from adequate protection safeguards.

ICO deadline for implementing UK addendum to EU SCCs / IDTA

UK organisations faced a deadline to update their existing data transfer arrangements to use either the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

EDPB Publishes New FAQs on Data Privacy Framework

The EDPB published two FAQ papers on the EU-U.S. Data Privacy Framework (**DPF**), providing clarity to organisations wishing to transfer personal data to the United States under the framework as a data exporter. For more information, read our insights on the topic here.

Dutch DPA fines Uber €290 million

The Dutch Data Protection authority imposed a fine of €290 million on Uber, finding that Uber had transferred personal data of European taxi drivers to the United States and failed to appropriately safeguard the data regarding these transfers, constituting an infringement of the GDPR. This was the third GDPR fine that the Dutch authority has imposed on Uber.

European Commission publishes periodic review report of DPF

On 9 October 2024, the European Commission published a report on the first periodic review of the adequacy decision of 10 July 2023, which had determined that the DPF provided an adequate level of protection for personal data transferred from the EU to the U.S. under the GDPR. The next periodic review will be carried out in three years.

2025 Trends

Possibility of challenge to the EU-US DPF

The DPF, in 2025, could face significant scrutiny and potential challenges. Privacy advocates, particularly Max Schrems, are expected to continue their efforts to challenge the framework, potentially leading to a "Schrems III" case. Schrems' concerns focus on whether US surveillance practices and redress mechanisms for EU citizens meet the requirements set by the CJEU.

The DPF includes measures to address these issues, such as limiting US intelligence agencies' access to data and establishing a Data Protection Review Court (**DPRC**) for EU citizens' complaints. Changes in administration in US politics and subsequent changes in policy could impact the DPF's implementation and enforcement. For example, a future administration prioritising national security over data privacy could increase surveillance activities, undermining the framework's adequacy.

In 2025, we can expect continued legal and political debates over the DPF's effectiveness and compliance with EU standards, but again despite an evolving political backdrop in the U.S., the EU places major importance on the protection of the rights of its data subjects and continues to pursue that agenda through the measures mentioned above. The European Commission has indicated that any challenge to the DPF will be robustly defended.

UK Adequacy Decision (Non-)Renewal

Under the GDPR, adequacy decisions are 'living instruments' and must be periodically reviewed by the EU Commission. In 2021, the EU Commission approved data transfer adequacy decisions to enable data transfers to the UK under the EU GDPR and the Law Enforcement Directive. In 2025, the EU Commission will be required to review the UK's adequacy status, which may be extended for up to four more years. However, significant divergence in data protection standards could lead to non-renewal, which would impact data flows and increasing costs for businesses. Controllers will be looking ahead to 27 June 2025 (the renewal date) closely to assess whether the UK decisions will be renewed.

New Adequacy Decisions

In 2025, new adequacy decisions (e.g. for Chile and Brazil) will likely reflect evolving global data protection standards and geopolitical dynamics and with this we can possibly expect to see increasing fragmentation of regulatory landscapes, driven by domestic political agendas rather than international coordination. This could lead to varied implementation of data protection rules across different regions, complicating compliance for multinational companies.

3. Protection of children's personal data

2024 was a year in which the protection of children's rights remained at the fore, with the adoption of the Online Safety Code by the national media and broadcasting regulator, Coimisiún na Meán. With the growth in the use of online technologies in society by children, the emerging EU regulatory framework aimed at protecting children's activities online identifies that there is a need for increased protection and safety.

February

DSA comes into effect for all intermediary service providers

The Digital Services Act (**DSA**) came into effect for all online intermediary service providers. As part of these obligations, e-commerce companies must put safeguards and appropriate measures in place to secure a high level of privacy, safety and security for minors. For more information on the DSA, see our previous article here.

July

Protection of Children (Online Age Verification) Bill 2024 (Bill 57 of 2024)

The draft Protection of Children (Online Age Verification) Bill 2024 (**Bill**) completed the second stage in the legislative process. The draft Bill imposes obligations on internet service providers to ensure that access to pornographic material on the internet be subject to an age-verification requirement (amongst other things).

October

Coimisiún na Meán publishes Online Safety Code

Coimisiún na Meán published its Online Safety Code, which sets binding rules applying to video-sharing platforms who have their EU headquarters in Ireland. The Code introduces obligations on these platforms to protect children from harmful video and associated content, including prohibiting the uploading or sharing of harmful content on their services, including cyberbullying and promotion of self-harm.

December

DPC publishes "Data Protection Toolkit for Schools"

The Data Protection Commission of Ireland (**DPC**) published a Data Protection Toolkit for Schools which will serve as a resource dedicated to further assisting schools in meeting their data protection obligations when processing the personal data of children. The toolkit includes guidance on aspects of data protection specific to schools, an FAQ section, and an appendix containing further resources.

2025 Trends

Age verification measures

In 2025, we can expect increased collaboration between regulators and industry stakeholders to develop standardised frameworks for age verification and content regulation. These efforts will aim to create a safer digital environment for children, aligning with evolving data protection standards and ensuring that both parents and children understand the importance of these measures.

Parental consent remains a critical element for online platforms to maintain for children under 16 to ensure their data is processed lawfully. Age assurance measures are likely to become robust, driven by the Digital Services Act and Online Safety and Media Regulation Act. There will also be a focus on preventing minors from accessing inappropriate material, with stricter controls and transparency from service providers. This is being explored on a national and EU level.

Expected EDPB guidelines on processing of children's personal data

In 2025, the EDPB is expected to release guidelines on processing children's personal data, reflecting evolving privacy concerns and technological advancements. These guidelines will likely emphasise stricter age verification measures to ensure that children's data is processed lawfully and transparently. The guidelines may also address the need for enhanced parental consent mechanisms, ensuring that parents are fully informed and involved in their children's online activities. Additionally, there will be a focus on protecting children's data in the context of emerging technologies, such as artificial intelligence and digital platforms, to prevent misuse and ensure compliance with the GDPR.

Following the TikTok decision in 2023, in which a substantial fine was imposed by the DPC on TikTok for breaches of data protection laws involving minors, there has been a heightened focus on safeguarding children's data. It is therefore likely that 2025 will bring the development of a more comprehensive approach to child protection, combining regulatory enforcement with technological solutions to create a safer digital environment for children across the EU.

4. GDPR Enforcement & EU Digital Reforms Package

In 2024, we witnessed a targeted focus on the interplay between the GDPR and the EU digital reforms package (**TechReg**), and how this will play out practically at an operational level for organisations and other organisations that process personal data. As new regulation comes into effect, we will see questions presented to data protection authorities that will help organisations to understand the practical implications of TechReg and its interplay with the GDPR.

Key guidance and opinions of the EDPB focus on the emerging technology landscape and the regulation of 'Big Tech'. Further, other opinions and guidance demonstrated that data subject rights are a key facet to the emerging regulatory landscape. The EDPB, in its third coordinated enforcement action for 2024, chose to focus on the right of access by controllers under Article 15 of the GDPR. Decisions of the EU and Irish courts showed that data subject rights and the convergence of these rights with innovative technology is at the core of the regulator's central concerns.

January

The EU Data Act and Interplay with EU Act as part of the Digital Reform Package

The Regulation on harmonised rules on fair access to and use of data (**Data Act**) entered into force. The Data Act will increase legal certainty for companies and consumers engaged in data generation, prevent contractual imbalances that impede data sharing, and apply new rules setting the framework for effective switching between different data service providers. The Data Act will become applicable in September 2025.

April

EDPB opinion on "Pay or OK" consent models applied by large online platforms

The EDPB adopted its Opinion 08/2024 on "Pay or OK" consent models applied by large online platforms. The EDPB was asked, under what circumstances and conditions 'consent or pay' models relating to behavioural advertising can be implemented by large online platforms in a way that constitutes valid, freely given consent. See our article on the Opinion here.

EDPB introduces new rules for GDPR's 'one stop shop' mechanism

The EDPB adopted its Opinion 04/2024 as requested by the French data protection authority on the notion of the main establishment of a controller in the EU. The Opinion considered the criteria for the application of the '*one-stop-shop*' mechanism controlling a controller's '*place of central administration*' in the EU. In order for the controller's place of central administration to be considered a main establishment, it must make decisions on the purposes and means of processing personal data and have the power to have these decisions implemented. See our insights here.

September

European Commission publishes view on interplay between Data Act and GDPR

The European Commission published FAQs about the Data Act. The Commission stated that the GDPR is fully applicable to all personal data processing activities under the Data Act. While the Data Act does not regulate the protection of personal data per se, it enhances data sharing by establishing rules related to the access and use of data. Ultimately, in the event of a conflict between the GDPR and the Data Act, the GDPR rules on the protection of personal data prevail.

October

EDPB opinion on certain obligations following from the reliance on processor(s) and sub-processor(s)

The EDPB published its Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s). The EDPB concluded (amongst other things) that controllers should have information on the identity of all processors and sub-processors *"readily available"* at all times, in order to best fulfil their obligations under Article 28 GDPR.

2025 Trends

Inter-regulatory approach to enforcement and supervision

To ensure the consistent, coordinated and appropriate enforcement and supervision of the EU's Digital Reforms Package, we can expect to see various national (and EU) regulators coming together in order to triage complaints and potential actions of non-compliance. For example: to the extent that a breach under the AI Act concerns a purely data protection issue, it is likely that such a matter will be managed by the DPC following an inter-regulatory consultation process. This position is further anticipated given the DPC's designation as one of nine authorities designated to safeguard fundamental rights under the AI Act. This trend is also reflected by the DPC's establishment of a new inter-regulatory affairs unit. Read more insights here.

Digital Reforms Package – continued implementation of legislation

The plethora of legislation contained in the EU Digital Reforms Package including the AI Act, NIS2, DORA, and the Data Act will need to be reviewed alongside the GDPR. Practical considerations in the ever-evolving world of technology and digital platforms will likely need to be addressed by the EDPB, to ensure that companies in the EU can continue to adopt groundbreaking technology whilst ensuring that the privacy rights of data subjects are protected. In 2025:

- the Data Act will be applicable from 12 September, meaning entities will need to consider their potential roles as 'data holders';
- DORA has been effective since 17 January 2025. DORA aims to enhance the digital resilience of financial institutions by addressing Information and Communication Technology risks. For more information on DORA, read our insights and listen to an overview in our podcast here.

More guidance on Data Subject Rights

We expect to see more guidance issued by the EDPB relating to data subject rights over the coming year. In October 2024, the EDPB selected the right to erasure ("the right to be forgotten") by controllers as the topic for its fourth Coordinated Enforcement Action. As such, national data protection authorities will co-ordinate their actions to generate analysis into the topic allowing for targeted follow-up on both national and EU level. As such, we expect to see increased activity in this area.

2025 Trends

Gamification/adaption of GDPR compliance

The joint WhatsApp decision of the EDPB and the DPC in 2021 emphases the need for clearer, more engaging ways to provide the transparency information contained in Articles 13 & 14 of the GDPR. Increasingly, entities are struggling with the task of ensuring that their transparency notices are provided to data subjects in a *"in a concise, transparent, intelligible and easily accessible form"*.

A possible trend we may see in 2025, is that the adaptation of GDPR compliance will increasingly incorporate gamification techniques to encourage data subject engagement. This involves using game-like elements, such as progress bars, rewards, and interactive tutorials, to make a compliance process more engaging and user-friendly. It is arguable that this approach could help data subjects better understand their data subject rights and other mandatory information contained in the GDPR.

5. Artificial Intelligence and Data Protection

In 2024, the final text of the AI Act was published. While the AI Act's application has a staggered approach, it regulates various categories of AI systems. The regulation of AI systems is multi-faceted. For AI systems which process personal data (at any stage in the AI lifecycle), the GDPR will apply, in addition to the AI Act.

As such, when developing or deploying an AI model or system which processes personal data, organisations will need to comply with the AI Act, the GDPR and other legal frameworks (e.g. intellectual property, copyright, etc.). We can expect to see continued guidance from data protection authorities on the AI Act's application and implications.

August

AI Act Comes into force

On 1 August 2024, the AI Act came into force. The Act introduces a uniform framework across the EU and prohibits certain AI practices due to their potential to cause significant harm or infringe fundamental rights. Additionally, the Act classifies certain systems as high risk and imposes obligations on providers to maintain technical documentation, implement a quality management system, ensure data governance, and conduct conformity assessments. For more information, see William Fry's AI Guide to the AI Act here.

The DPC welcomes X's agreement to suspend its processing of personal data for the purpose of training AI tool 'Grok'

In September 2024, the DPC welcomed X's agreement to suspend its processing of personal data contained in the public posts of X's EU / EEA users between May and August 2024 for the purpose of training its AI tool, 'Grok'. This was the result of the DPC's ex parte application to the High Court under section 134 of the Data Protection Act 2018, marking the first time the DPC relied on this interim legislative power.

September

Case C-203/22 (Dun & Bradstreet Austria) considers automated decision-making

Case C-203/22 concerned a mobile phone operator who refused to enter into a contract with an individual due to an alleged lack of creditworthiness (which was determined by Dun & Bradstreet). The individual requested to obtain information on the logic involved in the automated decision performed by Dun & Bradstreet to produce their credit score. The Austrian data protection authority ordered the disclosure of that information. The Advocate General held that while data subjects are not automatically entitled to information in respect of an algorithm used (i.e. trade secrets about how it works), but *"meaningful information about the logic involved"* within the meaning of Article 15(1)(h) of the GDPR must be given to individuals to the extent their personal data are processed so that they can understand how a decision was made impacting them.

October

EDPB Legitimate Interest Guidelines

In October 2024, the EDPB issued Guidelines 1/2024 on processing of personal data based on the legitimate interest of controllers. The Guidelines state that, for processing to be based on Article 6(1)(f) GDPR, three cumulative conditions must be fulfilled: (1) the pursuit of a **legitimate interest** by the controller or by a third party (which is must be lawful, present and not merely speculative); (2) the processing of personal data for the purposes of the legitimate interest(s) must be **necessary** (i.e. processing must be more than useful in achieving the legitimate interest pursued); and (3) the legitimate interest must not be overridden by the interests or fundamental rights and freedoms of the data subject (the '**balancing exercise**') (i.e. the controller must ensure that the processing activities do not have a disproportionate impact on the interests, rights and freedoms of stakeholders). For more insights on these guidelines, please see our article here.

December

EDPB AI Models Opinion

In December 2024, the EDPB issued Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, in response to a request by the DPC under Article 64(2) GDPR. In the context of AI models processing personal data, the Opinion addresses: (1) when and how an AI model can be considered as '*anonymous*'; (2) how controllers can demonstrate reliance on the legal basis of legitimate interest during the development (3) deployment phases of an AI model; and (4) the consequences of the unlawful processing of personal data in the development phase of an AI model on the subsequent processing or operation of the AI model once deployed. For more information on the Opinion, please see our insights on the topic here.

2025 Trends

AI and GDPR interplay

- Expect for providers and deployers of AI systems to grapple with, not only the AI Act, but also its interplay with the GDPR.
- Following the EDPB's Opinion on AI models, it is clear that controllers need to determine data protection issues objectively on a "case-by-case" basis taking into account the context of the processing. Deployers and developers need to make substantial contractual, technical and organisational efforts to demonstrate any level of compliance in both the development and deployment stages of AI models which process personal data (including by way of comprehensive documentation).
- While the EDPB's Opinion on AI models answered the DPC's 4 questions about AI models which process personal data, the EDPB's more detailed guidance on the interplay between the GDPR and AI will be hugely anticipated and the expectation is that it deals with challenging areas such as: special category personal data, purpose limitation, automated decision-making and more.

AI literacy

This requirement under the AI Act will be a critical focus area as these rules (along with those on prohibited AI systems) become law from 2 February 2025. From 2 August 2025, the rules relating to general purpose AI systems will take effect. For more insights, read William Fry's AI Guide here.

6. Cybersecurity and GDPR

With society's increased reliance on technology, and as the technology available to us becomes more advanced, so too do cybersecurity threats. In 2024, there were significant fines for personal data breaches imposed by the DPC. 2024 also saw an influx of legislation aimed at ensuring organisations within certain sectors implement minimum cybersecurity standards. Organisations saw the need to implement robust cybersecurity frameworks to detect, respond to, and remediate cyber incidents effectively.

May

DPC Protection Commission publishes 2023 Annual Report

The DPC published its Annual Report for 2023. In 2023, the DPC issued 19 finalised decisions resulting in the imposition of administrative fines totalling €1.55 billion on providers. Further, the DPC received 6,991 valid GDPR data breaches, a 20% increase on the number of breaches reported in 2022.

September

DPC fines Meta €91 million for data breach

The DPC announced its final decision following an inquiry into Meta Platforms Ireland Limited, following notification by Meta to the DPC (in 2018) that it had inadvertently stored certain passwords of European users in 'plaintext' (i.e. without any form of encryption or cryptographic protection). The decision resulted in the imposition of corrective powers and a fine of €91 million.

October

Cyber Resilience Act adopted

The Council adopted the Cyber Resilience Act (**CRA**), a new law on cybersecurity requirements for products with digital elements. The CRA introduces cybersecurity requirements for the design, development, production and making available on the market of hardware and software products on an EU-wide basis. The products under the scope of the regulation are those which are connected either directly or indirectly to another device or network. The CRA became effective on 10 December 2024.

Ireland misses NIS2 transposition deadline

The NIS2 Directive is an EU-wide piece of legislation on cybersecurity which updates the 2016 NIS 1 Directive and has been effective since October 2024. Key elements of the NIS 2 Directive are that it broadens the scope of in-scope entities and mandates minimum cybersecurity governance standards for such entities, including an all-hazards approach to cybersecurity risk-management measures and incident reporting obligations. It also established new supervisory and enforcement powers on Member States. Please visit our website for more insights about NIS 2. To date, Ireland is late introducing its national legislation to transpose NIS 2 into Irish law.

2025 Trends

NIS 2

We will await the transposition of this directive into Irish law in 2025. It is expected that the General Scheme of National Cyber Security Bill will be re-tabled and brought through Ireland's legislative process. While Ireland is late with transposition, organisations should continue with compliance efforts to understand if they are in-scope and, if so, begin to implement risk management systems and ensure that management boards receive the necessary cybersecurity training. Keep an eye out for more updates from our team.

Be cyber ready

As technologies in the AI space continue to develop and evolve, we can expect that organisations will (continue to) experience increased cyber threats and the need to be proactive and reactive in responding to such threats.

Contact us

For more information on any of these developments or data protection advice, please contact Leo Moore, Rachel Hayes, or your usual William Fry contact.

Leo Moore
PARTNER
Head of Technology
+353 1 639 5152
leo.moore@williamfry.com

Rachel Hayes
PARTNER
Technology
+353 1 639 5218
rachel.hayes@williamfry.com

Jordie Sattar
ASSOCIATE
Technology
+353 1 489 6533
jordie.sattar@williamfry.com

Paul Convery
PARTNER
Litigation & Investigations
+353 1 639 5193
paul.convery@williamfry.com

Adele Hall
SENIOR ASSOCIATE
Litigation & Investigations
+353 1 6395 163
adele.hall@williamfry.com

Niamh McCabe
SENIOR ASSOCIATE
Litigation & Investigations
+353 1 639 5089
niamh.mccabe@williamfry.com