Data protection newsletter

Issue 19

Given the publication of the AI Act in the Official Journal of the European Union, the clock is now running to deliver compliance on a stepped basis until full implementation of the AI Act in August 2026. In this issue we delve into the AI Acts requirement for a fundamental rights impact assessment. In addition, we consider the EDPB's recent publication on AI Auditing. Finally, we highlight some of the key messages from the DPC's annual report.

The AI Act is finally here

On the 12 July 2024, the much-anticipated EU AI Act was published in the Official Journal of the European Union, making it law on the 2 August. Much like the GDPR, it will take two years to be fully enforced, but also has a phased approach to enforcement, tackling the higher-risk areas first. Here is a brief timeline of key milestones:

July 2024
Published
The AI Act is published in the OJEU

August 2024
Enacted
Becomes law

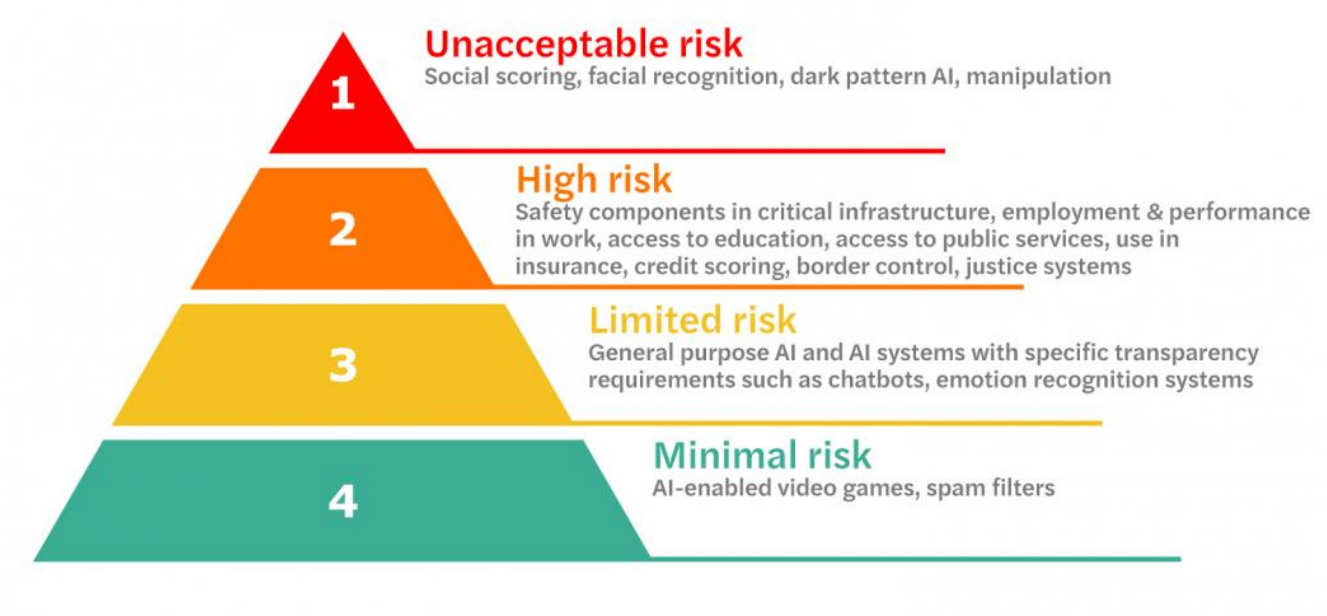
Feb 2025
Banned AI
Unacceptable risk systems are banned. Fines of 7% global turnover or €35 mil

July 2025
General purpose
Providers of GPAI must meet their obligations.
Codes of conduct published
National authorities selected

July 2026
High risk AI systems
Rules regarding high risk AI systems are in place. Fines for non-compliance

With the AI Act now providing clarity on its content, requirements and timeline, organisations are urged to initiate their compliance preparations. This compliance programme, when integrated into a comprehensive AI governance framework, will serve as a crucial tool to effectively manage AI usage within the organisation, ensuring its safe, responsible and efficient deployment.

See the full text of the Act here. The Act identifies different levels of risk associated with AI systems:



See here for more information on the risk levels.

There are different risk levels and different roles involved. Much like the GDPR (where we have controllers and processors) we have providers, deployers, distributors and importers in the AI Act. With all these roles and different responsibilities, it is vital to understand what role your organisation plays in the use and development of AI.

Key action: Establish your AI Governance framework

Fundamental Rights Impact Assessment

The AI Act has introduced an obligation to carry out a Fundamental Rights Impact Assessment (FRIA) in certain situations. A FRIA, a protective measure, is aimed at safeguarding an individual's fundamental rights from the adverse effects produced by an AI system. The main goal of completing a FRIA is to identify the risks to the rights of individuals likely to be affected and identify measures to be taken in the case of these risks materialising.

High-risk AI systems referred to in Article 6(2) of the EU AI Act are subject to the requirements of a FRIA, underscoring the crucial role of certain types of deployers of the AI system, including:

- Deployers that are bodies governed by public law.
- Deployers that are private entities providing public services.
- Deployers of high-risk AI systems are used to evaluate the creditworthiness of natural persons, establish their credit score, or assess risk and prices in the context of life and health insurance. (point to note: this covers both public and private entities).

A FRIA should be completed on the first use of a high-risk AI system, similar to the timing of a Data Protection Impact Assessment (DPIA) under the GDPR; it is recommended that the FRIA be completed in the AI system's development phase. This will become applicable from August 2026.

The EU AI Act refers to the below elements which should be included when completing a FRIA:

a) **Description:** of the high-risk AI system, its intended purpose(s), timeframes and affected people.

b) **Assessment:** of the specific risks of harm likely to impact the affected people.

c) **Risk treatment:** measures to address such risks, supplemented by a description of the implementation of human oversight measures.

The process for a FRIA and a DPIA is somewhat similar but differ substantially in their scope. A DPIA focuses on the rights and freedoms of data subjects affected by the processing of their personal data, whereas FRIA also concerns risks associated with non-personal data. The EU AI Act addresses the possible overlap of the two, where some obligations are already met through the DPIA, as such the FRIA will complement the DPIA. This will mean that a DPIA and FRIA may be conducted together and may even result in a single integrated report.

Once the FRIA has been completed, the deployer needs to notify the designated market surveillance authority of the results of the assessment by submitting its documented FRIA as part of the notification.

Key action: If you wish to deploy an AI system and fall within the scope, you need to complete a FRIA. Also, make sure to update your DPIA templates and processes to ensure risks related to AI are captured and mitigated.

GDPR compliance of AI systems

Recently the European Data Protection Board (EDPB) with the support of the Poll of Experts Programme, launched an AI auditing project which provides a comprehensive checklist for auditing AI systems and applications, focusing on their impacts and compliance with data regulations. The document provides a detailed methodology in the form of a checklist to perform an audit of an AI system. It emphasises the importance of transparency and accountability in AI systems.

The document discusses the concept of algorithmic auditing, which in simple terms is a method to inspect AI systems in specific contexts. It's a way to check how these systems work and what impacts they might have. This is important not just for regulators and the wider society who can use audit reports to assess AI systems, but also for those developing and using AI systems. The guidance emphasises that AI audits are key tools for ensuring that AI systems are accountable, transparent and comply with regulations.

The AI audit checklist is specifically focused on the impacts of AI. It's designed to check that AI developers and implementors have taken all necessary measures to ensure that their systems align with existing laws, such as the GDPR. It can assist organisations who are looking to introduce an AI system into their day-to-day operations as it will help them determine if the AI system is compliant with GDPR.

The guidance discusses the AI auditing process in detail, including the use of a model card, system map and the identification of moments and sources of bias.

A model card is a document designed to compile information about the training and testing of AI models. The EDPB guidance states that auditors should ask developers for the model card, as it will give an overall picture of the AI system. It will also enable auditors to determine any legal issues that need to be further explored before the AI system is integrated into the business.

A system map puts the algorithm in context, establishing the relationships and interactions between an algorithmic model, a technical system and a decision-making process. The EDPB guidance states that a draft version of the system map can be done by auditors based on the information provided in the model car. A final version should be reviewed and validated by the developers to ensure its accuracy.

Identification of moments and sources of bias is a part of the audit which involves identifying potential biases that the AI system can generate throughout different stages of the AI lifecycle. The EDPB provide a set of questions to consider during the audit process.

The EDPB emphasise the importance of producing a public audit report. Three different types of reports can be documented:

- An internal report that captures the process followed, the issues identified and the mitigation measures that have been or can be applied.
- A public report where the system, the auditing methodology, the mitigation measures implemented and further recommendations, if any are documented.
- Periodic follow-up reports that test the effectiveness of the mitigation measures.

Although completing an AI audit is not mandatory, it is a key step to ensure that organisations can evidence accountability by assessing the data protection risks associated with the introduction of an AI system or application.

As well as this guidance document from the EDPB expert group, several data protection authorities have issued their guidance on the use of AI with the **ICO** and **CNIL** being two of the most proactive.

The challenge for privacy teams is to digest all of this guidance and apply it to the specific context and situation of the organisation. A great place to start is at the top with a good AI strategy and building blocks for a governance framework, that includes the privacy team.

Key action: Get in touch with our team if you need to complete an AI audit.

DPC 2023 Annual Report

In May, the Data Protection Commission (DPC) published its **2023 annual report,** with several interesting findings within. Below we provide a brief summary of some of these findings.

1. Case Studies

There are 30 case studies included in the report which provide in-depth insights into topics discussed throughout the report and demonstrate the DPC's regulatory approach concerning various data protection compliance issues. The case studies cover instances of unintentional publication of personal data, excessive data requests and improper data retention. Additionally, it highlights issues with third-party data, inappropriate fees and delays in responding to access requests. Erasure request cases highlight compliance issues across sectors such as real estate, employment, gambling and healthcare. Furthermore, it discusses CCTV usage and enforcement actions against companies for unsolicited marketing communications.

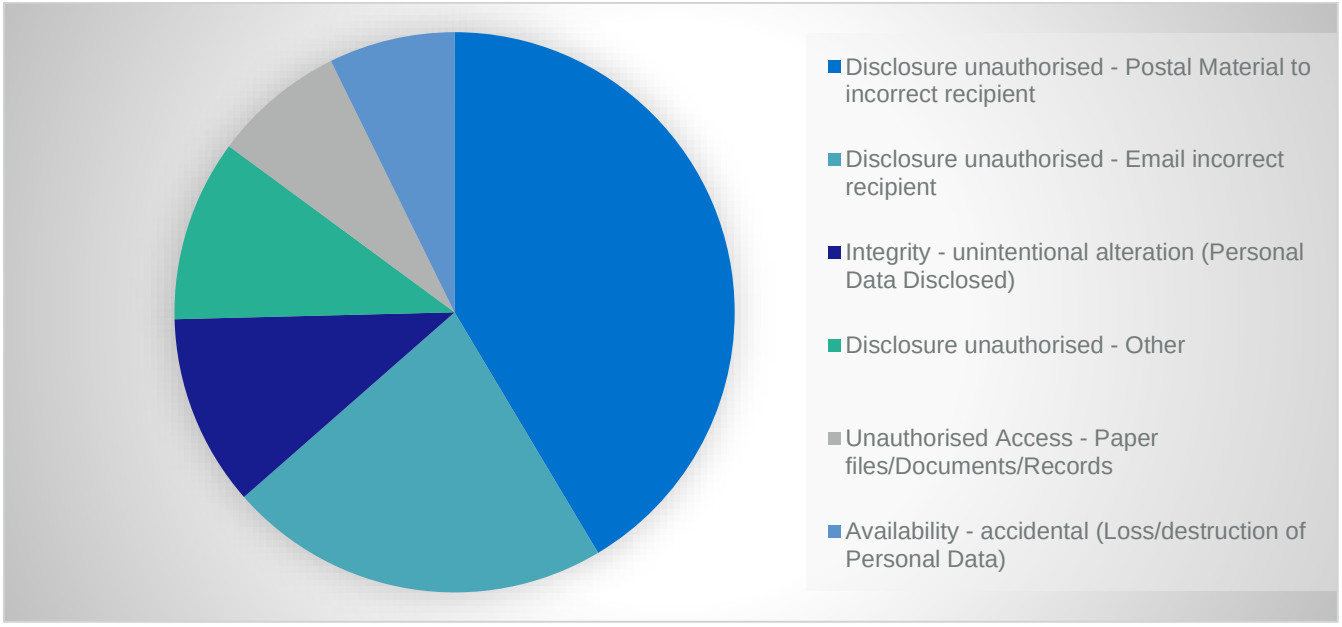
If you have identified a risk in these areas or are planning changes within these categories, analysing these case studies could be beneficial.

Page Number:	Case Study number:	Case Study Title:	Company Name/Type:	GDPR area:
71		Use of CCTV in a restaurant restroom	Aarval Limited	CCTV
77		Sporting Organisation and the Posting of Images of Children	Not named	Childrens Data Case Study
101	1	Organisation publishing alleged personal data	Property Website	General Accountability
102	2	Alleged unlawful retention and alleged unlawful processing in relation to a newsletter.	Property Management Company	General Accountability
103	3	Partial Compliance with a Rectification Request	Educational company	General Accountability
106	4	Complaint of excessive personal data requested by a letting agent	Letting agent	General Accountability
107	5	Access request seeking third party data	Not listed	Access Request
108	6	Access Request where a fee was requested	Medical Centre	Access Request
109	7	Failure to Respond to an Access Request	State Hospital	Access Request
110	8	Enforcement Notice Issued due to an Incomplete Response to an Access Request	Tusla	Access Request
112	9	Erasure Request Connected to a Property Sale	Real Estate Intermediary	Erasure Request
113	10	Complaint Related to Non-Compliance with an Erasure Request to a Prospective Employer	Not listed	Erasure Request
114	11	Non-compliance with an erasure request associated with an online gambling account	Bookmaker	Erasure Request
115	12	Non-compliance with an erasure request related to medical data	Healthcare provider	Erasure Request
117	13	Disclosure of health and financial data to a third party	State agency	Disclosure
119	14	Disclosure of personal data to a debt collection agency	Energy Service provider	Disclosure
121	15	Prosecution of Chill Insurance Limited	Chill Insurance LTD	Prosecution

Page Number:	Case Study number:	Case Study Title:	Company Name/Type:	GDPR area:
122	16	Prosecution of Hidden Hearing Limited	Hidden Hearing LTD	Prosecution
123	17	Prosecution of The Multiple Sclerosis Society of Ireland	Multiple Sclerosis Society of Ireland	Prosecution
124	18	Prosecution of Vodafone Ireland Limited	Vodafone Ireland LTD	Prosecution
125	19	Fair processing complaint relating to CCTV in the workplace	Beauty industry	CCTV
127	20	CCTV in Restrooms	Public Houses, Restaurants, Nightclubs & Transport Depots	CCTV
128	21	Breach Complaint related to employment information	Not named	Breach

2. Breaches

In 2023, the DPC received 6,991 valid GDPR data breaches, representing a 20% increase from 2022. 3,766 of these breaches related to the private sector, 2,968 to the public sector and 257 coming from the voluntary and charity sector.



3. Complaints

Between 1 January 2023 and 31 December 2023, the DPC received 11,200 new cases with 2,600 advancing to the formal complaint-handling process. This represents a 20% increase on the 2022 total and marks the highest number of cases received by the DPC since the GDPR came into effect.

Below we have set out the most frequent topics of complaints.

In 2023, the DPC received 230 complaints relating to electronic direct marketing and four companies were prosecuted for the sending of unsolicited marketing communications to individuals without consent.

Topic of complaints received	No	% of total
Access Request	1014	39%
Right to Erasure	374	14%
Fair Processing	348	13%
Direct Marketing	323	12%
Disclosure	121	5%

4. Enforcement Action

In 2023, the DPC issued 19 finalised decisions, resulting in administrative fines amounting to €1.55 billion, in addition to reprimands and orders.

Organisations	Fine Imposed	Key Actions for other organisations
Meta (Facebook)	€1.2 billion	Review your SCCs and Data Transfer Impact Assessments (DTIAs).
TikTok	€345 million	Companies must ensure when implementing new projects that they consider data protection by design and default
WhatsApp Ireland Ltd	€5.5 million	Companies must ensure that the legal basis upon they process information is valid.
Bank of Ireland	€750,000	Companies must ensure the implementation of appropriate technical and organisational measures to safeguard the integrity, confidentiality and security of customer data.
Centric Health	€460,000	Companies must implement robust technical and organisational measures to prevent and respond to ransomware attacks, ensuring appropriate security of personal data and maintain comprehensive documentation to demonstrate compliance.
Kildare County Council	€50,000	Companies must ensure they have a legal basis for collecting personal data via CCTV cameras. They must maintain transparency and implement necessary security measures and conduct regular assessments.
Department of Health	€22,500	Companies must ensure that data processing activities are necessary, proportionate, and aligned with the purpose for which they were collected, avoiding excessive and disproportionate data collection.

Key action: Review internal SAR procedures as this is an area with the highest complaints. Identify if additional controls can be put in place to reduce the likelihood of a complaint.

GDPR Survey

We recently completed our **annual GDPR survey** in partnership with McCann Fitzgerald. The webinar of the survey launch event can be accessed **online** and features a discussion with industry experts and Ireland's Data protection Commissioner, Graham Doyle. Following the results, Consulting partner Liam McKenna featured on Newstalk's Business Breakfast show, where he discussed the report's findings and the impact of GDPR six years on since it's implementation. You can listen to the full segment **here**.

Liam McKenna
Partner
lmckenna@mazars.ie

David O'Sullivan
Senior Manager
DOSullivan@mazars.ie

Lisa Clarke
Manager
Lisa.clarke@mazars.ie

Forvis Mazars in Ireland is a leading international audit, tax, advisory and consulting firm. Operating as a united partnership, Forvis Mazars works as one integrated team, leveraging expertise, scale and cultural understanding to deliver exceptional and tailored services in audit, assurance, tax, consulting, financial advisory, corporate finance and financial outsourcing. With 37 partners and 800+ staff based in Dublin, Galway and Limerick, the Irish firm draws on the expertise of more than 40,000 professionals in over 100 countries to assist major international groups, SMEs, private investors and public bodies at every stage in their development.

forvismazars.com/ie