Data protection newsletter
Issue 23

The first quarter of 2026 has been exceptionally busy in the data protection world with a range of new complaints, guidance and court cases to be dissected and assessed for impacts on compliance frameworks. Many clients and other organisations, are actively pursuing AI which is resulting in DPOs and compliance teams being involved in AI assessments and DPIAs, adding to the already full workload.

European Data Protection Board (EDPB) guidance, opinions and enforcement action

EDPB work programme

The EDPB Work Programme 2026–2027 sets out the Board's priorities for strengthening consistency across the EU and supporting organisations that find GDPR compliance challenging in practice. The programme builds on the EDPB Strategy 2024–2027 and focuses on areas where regulators continue to see inconsistent approaches, including anonymisation, pseudonymisation, legitimate interest, children's data, consent-or-pay, scientific research and rights under the Law Enforcement Directive.

A central theme of the programme is the development of practical tools that reduce the operational burden of GDPR compliance. The EDPB plans to publish templates for legitimate interest assessments, records of processing activities, privacy notices, breach notifications and DPIAs.

The programme also aligns with broader regulatory work such as the EDPB-EDPS joint opinion on the European Biotech Act, demonstrating the Board's focus on emerging technologies and evolving legislative frameworks. Read our detailed EDPB breakdown **here.**

Key action: New EDPB guidance and templates may alter existing compliance practices. Organisations should prepare to update documentation and processes and manage change carefully as templates begin to influence supervisory authority expectations.

Coordinated enforcement action – right to be erasure / be forgotten

The EDPB's 2025 coordinated enforcement action examined how organisations across 32 supervisory authorities implement the GDPR right to erasure. The findings highlight a number of operational weaknesses that continue to affect compliance. Many organisations lacked clear internal procedures, resulting in delays, missed deadlines and inconsistent responses. In several jurisdictions, individuals were not given adequate information about how to submit requests, what legal conditions apply or how decisions are made.

Supervisory authorities also identified issues with the misuse of anonymisation as a substitute for deletion. In many cases, methods described as anonymisation were reversible, meaning the data remained identifiable. Retention practices were found to be unclear or poorly justified, and automated deletion mechanisms were often missing. Technical challenges also arose when controllers attempted to delete data stored in backups, particularly in older systems that were not designed for granular erasure.

Training gaps and manual workflows created further risk. Staff were not always aware of their obligations and, in some cases, erasure requests were overlooked during internal transitions. The Irish case study demonstrated how a simple process change resulted in a missed request. Read our detailed EDPB breakdown **here.**

Key action: Ensure that you have the ability to meet right to erasure requests. Identify where they may be applicable and build relevant processes. Generally, improve processes for managing data subject rights requests. Note: at Forvis Mazars we are building automation into our processes using easy to access tools.

Coordinated enforcement action – transparency

The EDPB has chosen transparency as its 2026 coordinated enforcement focus. 25 supervisory authorities will assess how organisations meet their obligations under articles 12 to 14 of the GDPR. These investigations commonly begin with a questionnaire that examines how organisations inform individuals about their data, including through privacy notices and other communication channels. Depending on the authority, participation may be mandatory, and follow up actions may include guidance or enforcement.

The initiative will assess whether organisations provide information that is clear, accessible and tailored to the needs of data subjects. Regulators will refer to the Article 29 Working Party transparency guidelines, which remain the key interpretative reference. Common issues include overly broad wording, lack of clarity about lawful bases, insufficient detail on data sharing and notices that fail to explain processing in a layered or audience appropriate way.

The focus on transparency reflects its importance for enabling individuals to understand how their data is used and exercise their rights. It also encourages organisations to align documentation with current regulatory expectations, particularly as processing activities evolve. Read our detailed EDPB breakdown **here**.

Key action: Conduct a transparency audit, review privacy notices and ensure information supplied under articles 12 to 14 aligns with EDPB guidance.

Cookies and marketing: CNIL fine

TA recent CNIL decision highlights ongoing scrutiny of customer match and lookalike audience tools used for marketing. CNIL fined an organisation €3.5 million after it shared hashed data from more than 10 million loyalty programme members with a social media platform for targeted advertising. CNIL found that the organisation did not provide clear information about the data sharing and relied on bundled consent that did not meet GDPR requirements. It also failed to carry out a DPIA despite the scale and nature of the processing.

The decision reinforces the position held by regulators across Europe that organisations must explicitly inform individuals when their data is used for customer matching, including identifying the platforms involved. References in general privacy notices, or reliance on the platform's own disclosures, are not sufficient. Supervisory authorities continue to treat customer matching as high risk due to the involvement of large advertising platforms and the sensitivity of behavioural profiling, even when data is hashed.

The decision also aligns with wider enforcement themes such as transparency, consent specificity and the need to assess high risk processing in detail before implementation. You can read the full breakdown on CNIL fine **here.**

Key action: Organisations using customer match or custom audience tools should review whether their privacy notices clearly explain social media data sharing, assess whether existing consent mechanisms are sufficiently specific and determine whether a DPIA is required before deployment. Taking a proactive, regulator-aligned approach now can help reduce enforcement risk as scrutiny of digital marketing practices continues across the EU.

Lessons learned: University of Limerick fined €98,000

The University of Limerick case provides important lessons on the need for effective cybersecurity and clear governance. Between 2018 and 2020, the University experienced 12 data breaches, six of which resulted from successful phishing attacks. Attackers created convincing fake login pages, allowing them to access staff email accounts containing personal data relating to students, staff and third parties. The data included identity information, PPS numbers and some sensitive medical details.

The DPC found that the University's technical and organisational measures did not meet the requirements of articles 5(1)(f) and 32. Weaknesses included limited email security layering, the absence of domain based authentication and non mandatory cybersecurity training. Email filtering tools failed to detect malicious links embedded in images and MFA was not required for all users. Key policies were outdated or only introduced after the breaches occurred.

Further issues arose in the University's record of processing, several late breach notifications and delays in informing affected individuals. In some cases, individuals were only informed months after the initial report.

The DPC applied a €98,000 fine but noted that the University's cooperation and proactive improvements reduced the overall penalty. Read more on the fine **here.**

Key action: Gaps in technical and organisational controls, breach notification workflows, policies and training directly increase regulatory exposure. Organisations should test and continuously update these controls and processes.

European Biotech Act

The proposed European Biotech Act seeks to harmonise the regulatory framework for biotechnology, including clinical trials and emerging AI enabled life sciences applications. The EDPB and EDPS joint opinion supports the Act's aims but emphasises the sensitivity of health and genetic data processed in biotech environments. The opinion also supports the improved clarity on legal bases for processing special category data, stronger transparency obligations and safeguards for secondary use.

The proposal introduces a legal obligation as a new lawful basis for processing data required for clinical trials. This may reduce reliance on consent for data sharing although participants will still need to consent to take part in the trial itself. The opinion also clarifies roles within trials, confirming that sponsors are generally controllers, sites are processors and investigators are separate controllers. Clinical trial agreements will need to be updated to reflect these roles and include appropriate controller controller arrangements.

Retention rules are clarified, with only the master file required to be stored for 25 years. Other personal data should have separate, shorter retention periods. Regulators also highlight the need for default pseudonymisation, enhanced transparency and robust governance for any secondary use of trial data. Find our full guidance on European Biotech Act **here**

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

Data Subject Access Requests (DSARs) and why they exist

DSARs allow individuals to understand how their data is processed and support them in exercising other GDPR rights such as rectification and erasure. Recent case law provides clarity on the scope of the right and when requests may be refused. The Paris Court of Appeal confirmed that DSARs do not entitle individuals to copies of work emails they already know about, particularly where those emails contain only identity information. The purpose of the right is to allow individuals to verify the lawfulness and accuracy of processing, not to access broad sets of documents.

At EU level, the Brillen Rottler case provides a framework for identifying requests that may be abusive or excessive. Controllers may refuse a DSAR where they can demonstrate that the request is made for reasons other than verifying processing. Factors such as timing, the data subject's behaviour and the nature of the data may all be considered. The burden of proof remains high and must be supported by clear documentation.

These developments may be relevant in Ireland, where DSARs are often used before litigation and can place significant pressure on organisations. Read our full breakdown on DSARs **here.**

Key action: Review and update DSAR approval processes to ensure that abusive or excessive request are identified early and dealt with accordingly.

Developments in AI

General Scheme of the Regulation of Artificial Intelligence Bill 2026

On the 4th of February the Irish Government published the general scheme for transposing the EU AI Act into Irish law, see press release here: **General Scheme of the Regulation of Artificial Intelligence Bill 2026 - DETE**. Once law, this will be a vital piece of legislation for companies that are developing and deploying AI systems in Ireland. We were already aware of the different bodies that are going to be involved with AI regulation.

While it is early days in the political negotiation process it will be interesting to see what the final result is.

Key action: Keep an eye out for updates.

Ireland Digital and AI strategy

On the 18th of February the Department of An Taoiseach published a new landmark strategy on digital and AI from 2026 – 2030. It has some ambitious goals and focus points that will have an impact across society.

Some of the headline items include:

- Digitisation of 100% of key public services
- Establishing a new AI Advisory unit for public service
- New AI literacy campaigns
- AI sector champions and other sector specific initiatives
- AI Office of Ireland
- Hosting the AI and Digital Summit in October 2026 as part of the EU presidency.

For data protection professionals this will mean large scale changes and transformations that will result in numerous compliance activities and obligations, new risks emerging and enhancing existing risks. Importantly it also means that DPOs need to be able to understand the AI systems that are being introduced and the data protection obligations. Data Protection Impact Assessments are going to be needed on most occasions.

Key action: Public sector bodes are going to quickly catch up with the private sector in their use of AI. Data protection teams are going to have to upskill in order to understand the impact AI will have on data subjects and to complete DPIAs.

AI Act Omnibus

In March the European Conci and Parliament set out their respective negotiating positions for the AI Act Omnibus proposal with both bodies supporting the stop the clock. This is rapidly changing area with negotiations ongoing but as of writing the negotiating positions are:

- New fixed deadlines for the application of high-risk AI obligations. For Annex I systems it will be August 2028 and for Annex III systems it will be December 2027. This is a change from the current deadlines that are reliant on the release of specific guidance.
- Ban non-consensual intimate deepfakes which is something that hit headlines in a major way related the use of GROK on X.
- Reinstatement of the obligation to register a system that a provider deems as non-high-risk per Article 6(3) of the AI Act.

Key action: The AI Act might be stalled but organisation should continue on their AI governance journey in order to protect from other business and compliance risks while also enhancing the opportunity presented by AI.

Contacts

Liam McKenna
Partner
lmckenna@mazars.ie

David O'Sullivan
Director
DOSullivan@mazars.ie

Lisa Clarke
Senior Manager
Lisa.clarke@mazars.ie

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

forvismazars.com/ie