the dpia

GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE

The DPIA is an assessment of the impact of the most significant and important-to-know data protection issues from around the globe. It's not the full story, just a quick 3-minute read, collated and condensed to keep you updated with the latest news in our ever-evolving industry.

Governing AI agents: What organisations need to consider

For organisations deploying or considering the deployment of AI agents, questions around accountability, oversight, and risk are becoming increasingly pressing. As these systems act with greater autonomy across data, systems, and workflows, existing governance models are being tested in new ways.

In this blog, we explore what effective governance looks like for AI agents in practice. We examine how regulatory expectations differ across key jurisdictions and highlight the areas organisations should focus on to maintain control, manage risk, and deploy AI agents responsibly as regulation continues to evolve.

Read our blog

UNITED KINGDOM

ICO updates DSAR guidance following DUAA changes

The Information Commissioner's Office (ICO) has published the updated guidance to reflect stricter transparency and accountability requirements for Data Subject Access Requests (DSARs), introduced by the Data Use and Access Act (DUAA) 2025.
The revised guidance clarifies how organisations should approach DSAR handling in practice, particularly where requests are complex, high-volume, or require further clarification.

Key changes include:

- Controllers may ‘stop the clock’ where reasonable clarification is required
- Where a request is refused, data subjects must be informed of their right to raise a complaint directly with the controller
- The volume of data involved is a relevant factor when assessing whether a request is unreasonable or disproportionate

Read the updated ICO guidance

Council data breach highlights growing risk for Public sector organisations

The Royal Borough of Kensington and Chelsea has confirmed a ‘serious’ data breach affecting hundreds of thousands of individuals, following unauthorised access to internal systems. Sample data indicates that sensitive and personal information may have been accessed, although the council doesn’t believe third-party systems were compromised.

The incident illustrates the scale of cyber risk facing Public sector organisations. More than 150 local government incidents were reported to the Information Commissioner's Office (ICO) in 2024, and Kensington and Chelsea Council reported intercepting over 113,000 phishing attempts between June and September alone, highlighting both the volume and persistence of attacks on local authorities.

For organisational leaders, the breach underlines how persistent attack activity raises the risk of compromise, emphasising the importance of effective monitoring, staff awareness, and clear escalation pathways. **Read our blog** for tips on safeguarding your organisation against phishing.

EUROPEAN UNION

Irish DPC fine backlog highlights realities of GDPR enforcement

The Data Protection Commission (DPC) of Ireland has confirmed it is owed more than €4 billion in GDPR fines that cannot yet be collected, largely due to ongoing legal challenges. Under Irish law, administrative fines must be confirmed by the courts before enforcement can proceed, meaning collection is paused while appeals and confirmation processes are ongoing.

The situation highlights a key enforcement reality for organisational leaders: regulatory exposure does not end with the issuance of a fine. Lengthy appeal processes, sustained regulatory scrutiny, and associated legal and operational costs can persist for years. This reinforces the importance of robust documentation, defensible decision-making, and compliance frameworks that can withstand prolonged regulatory engagement.

The **DPC's Know Your Obligations guidance** offers practical insight into regulatory expectations and how organisations can demonstrate compliance in practice.

CNIL fines FREE Mobile and FREE €42M for GDPR violations

Issued on 13 January 2026, the enforcement action followed an October 2024 data breach that exposed sensitive financial data relating to approximately 24 million subscribers.

CNIL's investigation found that the companies:

- Failed to implement appropriate technical and organisational measures to secure personal data
- Did not communicate effectively with affected individuals following the incident
- Retained personal data for longer than necessary

The case reinforces the importance of robust data lifecycle governance, particularly around retention and deletion practices. Excessive data retention not only increases breach impact but can also form a standalone compliance failure. **Read our blog** on data retention and the GDPR for practical guidance on building compliant retention frameworks.

Dutch DPA fines university following major data breach

Autoriteit Persoonsgegevens (AP) has issued HAN University of Applied Sciences a €175,000 fine for GDPR violations following a cyberattack that exposed a wide range of personal data. The compromised information included personal and special category data, such as names, addresses, passwords, national identification numbers, and political preferences.

The AP's investigation found multiple security and governance failures, including inadequate mitigation of known SQL injection risks, excessive database access rights, poor password protection, and the absence of a deletion policy.

The decision reinforces that longstanding or well-known security weaknesses are unlikely to be tolerated by regulators, particularly where large volumes of sensitive or special category data are involved. Businesses should:

- Address known vulnerabilities promptly and proportionately
- Apply the least privilege principle to database and system access
- Implement and enforce clear data deletion and retention policies
- Use modern, secure password hashing and storage practices

For best practice tips on password management, **read our blog**.

CANADA & UNITED STATES

New York Governor signs RAISE Act into law

The Responsible AI Safety and Education (RAISE) Act introduces safety obligations for large developers of frontier AI models. The Act applies to organisations that train or deploy models using more than $100 million in computational resources and is designed to reduce the risk of large-scale or critical harm.

The Act requires in-scope organisations to implement documented AI safety and security measures, retain and disclose supporting records to regulators where required, and avoid deploying frontier models where risks cannot be adequately mitigated. It also introduces ongoing governance expectations, including periodic reviews, independent audits, and strict incident notification requirements.

With the RAISE Act's obligations set to apply from January 2027, **Michael McCagh, DPO at The DPO Centre**, stresses the importance of early preparation: *'Don't wait for enforcement. Draft your governance protocols, start your bias audits, map where AI touches your employment decisions, and establish clear policies for employees. Proactive compliance protects both your organisation and your workforce — worthwhile steps for any business using AI, whether the RAISE Act applies or not.'*

Read the RAISE Act

Canada's OPC reminds organisations of data deletion responsibilities

On 13 January 2026, the Office of the Privacy Commissioner of Canada (OPC) issued a reminder to organisations selling returned electronic devices about their obligations to protect personal information. The update follows an investigation into Staples Canada, which was found to have resold returned laptops without fully removing users' personal data. The incident highlights a clear operational risk: inadequate data sanitisation can lead to unintended disclosure of personal information and regulatory scrutiny.

In its guidance, the OPC underscored the importance of robust data deletion practices, including instructions to:

- Perform a factory reset using the manufacturer's instructions to fully wipe personal information from any electronic device before resale
- Provide employees with clear, consistent, and standardised instructions on how to remove personal information from returned devices
- Fully train staff so they can complete technical tasks related to securely wiping data from electronic devices

Read the OPC's press release

INTERNATIONAL

China's CAC publishes data protection Q&A

Published on 9 January 2026 by the Cyberspace Administration of China (CAC), the Q&A clarifies key data protection obligations under China's Personal Information Protection Law (PIPL). It focuses on areas where organisations commonly seek guidance and provides practical clarifications on:

- Definitions of personal and sensitive personal information, helping organisations classify data consistently and apply appropriate safeguards
- Personal information protection impact assessments (PIPIAs), including specific guidance on when and how to conduct such assessments for facial recognition and other biometric technologies
- Designation of a person in charge of personal information protection, including when this is required and how to submit the relevant information to the CAC

Read the Q&A

We are recruiting!

To support our ongoing requirement to continuously grow our remarkable and extraordinary **#ONETEAM**, we are seeking candidates for the following positions:

- **Data Protection Officers (United Kingdom)**
- **Data Protection Officers (The Netherlands)**
- **Data Protection Officers (EU)**
- **Data Protection Officers - Life Sciences (United Kingdom)**
- **Data Protection Coordinator - Life Sciences (Poland)**
- **Senior Commercial Executive (United Kingdom)**

If you are looking for a new and exciting challenge, and the opportunity to work for a **Great Place to Work-Certified™** company, **ranked in the top 50 of the UK's Best Workplaces™ for medium-sized businesses**, **apply today!**

FOLLOW US ON LinkedIn