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.

IT equipment disposal: How to stay GDPR compliant

For organisations managing IT equipment across multiple teams, sites, or suppliers, disposal is often treated as an operational task rather than a data protection risk. However, where personal data remains recoverable on retired devices, organisations may be unable to demonstrate GDPR compliance.

This blog explains the key risks linked to IT equipment disposal and the GDPR principles that apply. It covers practical decisions such as software wiping versus physical destruction, how to select compliant disposal providers, and the documentation needed to evidence secure, accountable data destruction throughout the equipment lifecycle.

Read our blog

CANADA & UNITED STATES

US Supreme Court to clarify scope of video privacy law

On 26 January 2026, the US Supreme Court agreed to hear a case that will determine who qualifies as a 'consumer' under the federal Video Privacy Protection Act (VPPA). The ruling could reshape privacy litigation, particularly where tracking technologies are used alongside video content, with statutory damages of up to $2,500 per violation.

The Court will decide whether the law applies only to people who subscribe to audiovisual services or more broadly to anyone who receives other services from a provider that also

offers video. A wider interpretation could significantly increase litigation risk for organisations that combine video with analytics or advertising tools.

The case highlights growing US litigation risk around tracking technologies and the need for clear governance where video content and third-party tools intersect. Organisations should consider:

- Reviewing tracking technologies used on pages that include video
- Mapping where video content appears across websites, apps, or emails
- Checking whether video-related data is shared with third parties
- Ensuring consent and opt-out controls cover video interactions

Track the ruling

OPC and CNIL sign cooperation agreement

The Privacy Commissioner of Canada (OPC) and France's data protection authority (CNIL) have signed a declaration of cooperation aimed at strengthening collaboration on emerging privacy challenges. The agreement builds on discussions held during the G7 meeting of data protection authorities in December 2025 and reflects growing international coordination around new technologies.

Under the declaration, the two regulators will work together on joint research, share regulatory strategies and investigative best practices, and organise workshops to address cross-border data protection issues. For organisations operating internationally, the agreement signals continued alignment between regulators and an increasing focus on coordinated oversight of evolving digital risks.

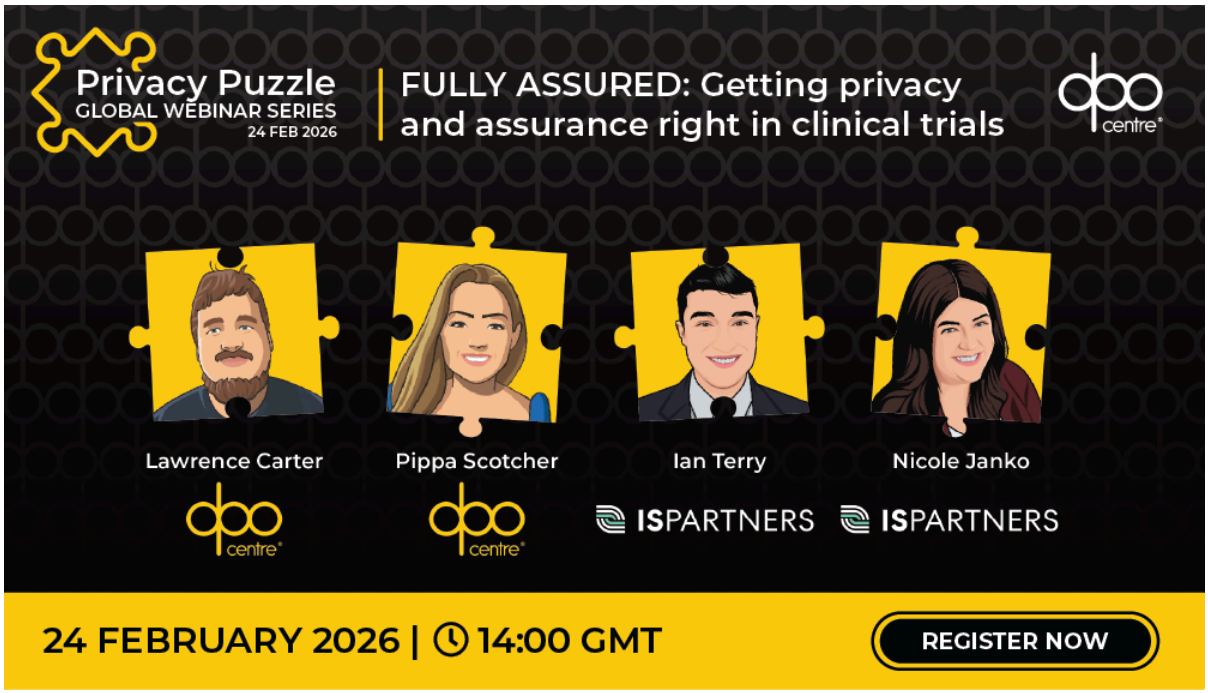
Read the declaration

Substack confirms data breach affecting user contact details

On 5 February 2026, newsletter platform Substack confirmed that an unauthorised third party accessed user data in an incident that occurred in October 2025. The breach data included email addresses, phone numbers, and certain internal metadata, but the company stated that more sensitive information, such as passwords, credit card details, and other financial data, was not affected.

Substack identified the issue in February 2026 and said the vulnerability has since been fixed, with an investigation underway. However, the four-month gap between the breach and its detection highlights ongoing concerns around security monitoring and incident response, reinforcing the need for effective detection capabilities, clear escalation processes, and timely investigations.

Read our blog for 5 tips for an effective breach management response.



UNITED KINGDOM

ICO publishes guidance on how it handles data protection complaints

The framework sets out how complaints are triaged, when the Information Commissioner's Office (ICO) will investigate in more detail, and how outcomes are determined.

Under the approach, the ICO will prioritise cases that involve significant harm, affect large numbers of people, relate to vulnerable individuals, or raise issues of wider public interest. Some complaints may be recorded for intelligence purposes only, helping the regulator identify trends, emerging risks, and organisations that show patterns of non-compliance.

For organisations, the framework reinforces the importance of resolving issues early, demonstrating compliance, and engaging constructively with the regulator, as repeated complaints or systemic concerns may trigger further scrutiny.

Read the guidance

EUROPEAN UNION

EDPB and EDPS raise concerns over Digital Omnibus proposal

On 11 February 2026, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a joint opinion on the proposed **Digital Omnibus Regulation**. Whilst both authorities support the goal of simplification, they raised significant concerns about amendments to the definition of 'personal data'. They warned the proposals could weaken protections, create legal uncertainty, and make data protection law harder to apply in practice. Both authorities have urged EU lawmakers not to adopt these changes, signalling that core GDPR concepts are likely to remain a key point of debate as the proposal progresses.

Read the Opinion

New EU procedural regulation enters into force

Regulation (EU) 2025/2518 sets out clearer timelines and processes for how data protection authorities (DPAs) handle cross-border complaints. The new rules will apply to enforcement actions opened after 2 April 2027.

The regulation is intended to make GDPR enforcement faster and more consistent across the EU. Key changes include:

- **Admissibility checks:** Complaints must contain specific information before proceeding
- **Early resolution:** DPAs may close cases quickly where the issue has already been fixed
- **Clear deadlines:** Simple cases should be resolved within 12 months and complex cases within 15 months (with one extension)
- **Stronger cooperation:** DPAs must share key documents, with rights for parties to be heard and access evidence

The new rules signal tighter timelines and more structured investigations, meaning less room for prolonged or fragmented cross-border enforcement processes.

Read the regulation

Dutch DPA sets out vision for responsible use of generative AI

Published by Autoriteit Persoonsgegevens (AP) on 4 February 2026, the document outlines how generative AI can be deployed safely, responsibly, and in line with fundamental rights. The paper explores future scenarios, technology trends, and the applicable legal framework, promoting a ‘values at work’ approach in which AI is developed and used with clear safeguards and oversight.

The AP highlights four priority areas for organisations deploying generative AI:

- **AI literacy:** Ensure board members and operational teams understand how the system works, its risks, and its impact on end users
- **Monitoring:** Track how the application behaves in practice, both through overall trends and targeted sample reviews
- **Information management:** Maintain strong control over data, access, storage, and cyber risks before introducing generative AI components
- **Dependency:** Assess supplier lock-in risks, including control over input data, model updates, security processes, and long-term flexibility

The AP's vision reinforces that generative AI must be governed in line with existing frameworks, including the GDPR and the EU AI Act, and that trust in the technology will depend on organisations embedding these safeguards from the outset.

Download the AP’s paper

INTERNATIONAL

Vietnam opens consultation on implementing decree for new AI law

On 6 February 2026, Vietnam’s Ministry of Science and Technology (MST) opened a consultation on a draft decree to implement the country’s new Law on Artificial

Intelligence, due to take effect on 1 March 2026. The decree sets out a comprehensive framework for the management, development, and deployment of AI, addressing risks linked to rapid adoption across sectors.

For organisations, the draft introduces:

- A risk-based classification model for AI systems
- Mandatory notification and monitoring through a national AI portal
- Labelling requirements for AI-generated content
- A regulatory sandbox for controlled testing of new AI tools

As the decree is required for the law to take effect, organisations developing or deploying AI in Vietnam should begin assessing how their systems may be classified and governed under the new framework.

Learn more

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)**
- **Data Protection Support Officers (United Kingdom)**

If you are looking for a new and exciting challenge, **apply today!**

FOLLOW US ON LinkedIn