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.

ISO:2025 update: What's changed and why it matters

In our latest blog, we explore the 2025 update to ISO 27701. The revised standard gives businesses a clearer, more credible way to show how privacy risks are managed in practice, not just in policy. It also helps teams build trust with customers and partners at a time when expectations for transparency and accountability are rising fast.

The blog covers what has changed, how the updates strengthen privacy governance, and where you should focus efforts to get the most from certification.

Read the full blog

CANADA & UNITED STATES

Canada launches register of AI uses in federal government

As part of the AI strategy for the federal public service, the Treasury Board has published the Government of Canada's first public AI register. The first edition lists more than 400 systems from 42 institutions, covering everything from early research to deployed operational tools. It includes details on purpose, use case, and whether each system was developed internally or by a vendor. Public consultations in 2026 will shape the next edition.

For organisations tracking AI governance, this strategy signals a continued shift toward clearer reporting and greater accountability for AI use.

See the Open Government Portal for details

G20 sets out shared priorities for AI governance without US participation

On 22-23 November 2025, leaders from major global economies met in Johannesburg for the G20 summit and adopted a declaration covering many global challenges. On responsible AI, the declaration outlined shared expectations for transparency, fairness, accountability, and human oversight, alongside safeguards for privacy, data protection, and data governance.

The United States did not attend and therefore did not sign the declaration, citing concerns about the process and the host nation. While the US has signalled it will prioritise AI when it hosts the G20 next year, their absence raised questions about how actively they plan to engage in shaping global AI practices.

For US organisations operating across borders, staying close to these developments will be key to maintaining alignment and meeting future compliance expectations.

California introduces new data breach deadlines

Under California's new data breach rules, taking effect on 1 January 2026, businesses and public bodies must disclose a breach within 30 calendar days, unless one of two exemptions applies. If more than 500 residents are affected, organisations must also submit a notice to the California Attorney General within 15 days of notifying consumers.

The update is designed to increase transparency and reduce delays that occurred under the previous 'in the most expedient time possible' standard. Regulators are signalling firmer expectations and penalties for late, inaccurate or incomplete notifications.

For organisations operating across multiple states, these changes reinforce the need for a comprehensive incident-response plan. This includes clear internal processes, updated notification templates, and strong coordination with any third-party providers. Keeping response plans aligned with varying state deadlines will be essential to managing risk and avoiding costly enforcement action.

UNITED KINGDOM

Concern over ICO's handling of major data breach

More than 70 civil-society groups, legal experts, and academics have called for a parliamentary inquiry into what they describe as a sharp decline in enforcement by the Information Commissioner's Office (ICO). Their demand was triggered by the ICO's decision not to investigate the MoD for a massive data breach that exposed the identities of more than 19,000 Afghan nationals fleeing the Taliban. The coalition warns that the ICO's softer approach weakens trust, increases risk, and leaves people and organisations exposed to growing security threats.

The matter is now under parliamentary scrutiny, with the public evidence session scheduled today, 10.30am, 9 December 2025.

Read our data breach management best practice tips

EUROPEAN UNION

Clinic fined for exposing client health data in messaging group

Spain's data protection authority, Agencia Española de Protección de Datos (AEPD), has fined a medical clinic €30,000 after it created a WhatsApp group for promotional messages and added around ninety clients without consent. Participants could see each other's phone numbers and, by association, their status as patients of a cosmetic clinic. The authority found this revealed special category health data and showed a lack of basic confidentiality measures.

The clinic had not assessed the risks of using a group messaging platform or put safeguards in place to prevent unauthorised access. While certain processing was lawful, it did not remove the duty to protect sensitive information, highlighting the need for stronger data protection controls.

[Read our blog on how data protection builds customer trust and loyalty]

NOYB complaint leads to penalty over cookie violations

France's Commission Nationale de l'Informatique et des Libertés (CNIL) fined the publishing company *Les Publications Conde Nast* €750,000 for placing cookies on user devices without valid consent. The case was brought to light by *noyb*, the European privacy rights group, which raised concerns about how vanityfair.fr handles trackers.

CNIL's audits found that cookies were installed as soon as visitors arrived on the site, and some were wrongly shown as 'strictly necessary' without a clear explanation. The options for refusing or withdrawing consent also did not work, as new cookies were still added, and existing ones remained active. The case highlights the need for clear and transparent information and reliable consent mechanisms.

INTERNATIONAL

India introduces new privacy regime

On 13 November 2025, India enacted its Digital Personal Data Protection Rules 2025, which operationalise the Digital Personal Data Protection Act 2023 (DPDPA) and cover key areas including privacy notices, consent managers, breach reporting, data retention, and the definitions and constitution of the Data Protection Board.

Implementation will be phased, with the definitions and creation of the Data Protection Board taking effect immediately. One year after publication, the rules for registering and the obligations of consent managers begin. After 18 months, all obligations apply, and companies operating in India must meet the full set of applicable requirements. The phased roll-out gives organisations time to prepare, but planning and compliance work should begin now.

[Read the Digital Personal Data Protection Rules 2025](#)

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)**

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

FOLLOW US ON LinkedIn