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.

GDPR compliance in white label banking

White label banking allows brands to offer financial services under their own name, without needing to build or operate a licensed bank themselves. But with that convenience comes the responsibility of managing data protection risks across a complex chain of partners. In our latest blog, we explore the GDPR risks in this multi-party model and outline practical steps for ensuring compliance.

From clearly defining controller and processor roles to handling DSARs and breach responses, businesses must work closely with banks and vendors to ensure transparency, accountability, and data protection at every stage. Read the full blog to understand your obligations and protect your customers.

Read our blog

UNITED KINGDOM

UK Employment Rights Bill amendments propose NDA ban

On 7 July 2025, the UK government published further amendments to the Employment Rights Bill that would ban non-disclosure agreements (NDAs) in cases involving workplace harassment and discrimination. Under the proposed reforms, confidentiality clauses that prevent individuals from speaking out about misconduct (including those in settlement agreements) will be unenforceable.

Importantly, NDAs used to protect legitimate commercial interests or intellectual property (IP) rights will still be permitted.

If passed, the amendments will have wider implications on data governance. Employers should:

- Update contracts and settlement templates to reflect the proposed NDA restrictions
- Document and store complaints and investigations securely, in line with the UK General Data Protection Regulation (GDPR)
- Train staff to spot when NDAs may unlawfully silence individuals
- Only collect information relevant to the complaint and apply clear retention rules

Learn more about the proposed amendment

ICO proposes new approach to cookie consent

On 7 July 2025, the Information Commissioner's Office (ICO) launched a call for views on a proposed new enforcement approach under Regulation 6 of the Privacy and Electronic Communications Regulations (PECR). Regulation 6 currently requires organisations to obtain user consent before storing or accessing information on a device (such as cookies), unless the activity is strictly necessary.

The ICO's proposal aims to enable privacy-preserving advertising models to operate without explicit user consent, where the risks are demonstrably low. Consent would still be required for targeted advertising involving personal data.

Alongside the consultation, the ICO has updated its Storage and Access Technologies (SATs) guidance to reflect changes introduced by the new Data Use and Access Act 2025. The revised guidance now permits consent-free use of cookies for specific low-risk purposes, such as site analytics and performance monitoring.

Have your say on the consultation, which is open until 29 August 2025.

EUROPEAN UNION

Commission publishes General-Purpose AI Code of Practice

On 10 July 2025, the European Commission published the final version of the General-Purpose AI Code of Practice – a voluntary framework designed to help AI developers comply with the forthcoming requirements of the EU AI Act.

The Code is structured around three core areas:

- **Transparency:** Introduces a user-friendly Model Documentation Form to help providers consolidate key technical and operational details in one place
- **Copyright:** Recommends practical steps to ensure model development complies with EU copyright law
- **Safety and Security:** Outlines risk management best practices for developers of the most advanced AI models where systemic risks may arise

The Code helps providers of multifunctional AI models demonstrate compliance with key AI Act obligations, helping to reduce administrative burden and increase legal certainty. Organisations will be able to sign the Code once it has been formally endorsed by EU Member States.

Read the Code

EDPB and EDPS welcome simplification of GDPR record-keeping

On 9 July 2025, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint opinion supporting the proposed increase in the GDPR's record-keeping exemption threshold from 250 to 750 employees (unless high-risk processing is involved). Part of the European Commission's fourth Omnibus package, the changes aim to ease administrative burdens for mid-sized organisations.

While welcoming the move, regulators stressed that simplification must not weaken accountability. They called for clarity on the 750-employee threshold and urged that public authorities remain excluded from the exemption.

Despite the changes, Records of Processing Activities (RoPAs) remain key to demonstrating compliance, and organisations must continue documenting high-risk activities. Businesses should continue to monitor legislative developments and ensure that high-risk processing is still appropriately documented and assessable by supervisory authorities.

Read the EDPB and EDPS joint opinion

Dutch DPA highlights oversight challenges in the digital age

On 14 July 2025, the Dutch data protection authority, Autoriteit Persoonsgegevens (AP), published a position paper outlining the growing challenges it faces in supervising GDPR compliance in a digitised society.

The paper highlights systemic risks, including online discrimination, mass surveillance, and dependency on non-EU digital services as key threats to data protection and fundamental rights. To address these risks, the AP aims to reduce uncertainty around GDPR compliance and promote better understanding and use of data subject rights.

However, the AP warned of significant internal constraints: limited capacity to initiate investigations, mounting delays in responding to complaints, and a backlog of unanswered guidance requests. It argues that these limitations undermine enforcement and regulatory clarity at a time when digital threats are rapidly increasing and is calling for greater structural investment to support its strategic priorities.

Download the AP's position paper

CANADA & UNITED STATES

New technology protects online content from AI crawlers

American internet infrastructure firm Cloudflare has announced new technology that allows websites to block AI bots from scraping their content without permission. Already active on over a million sites, the system targets AI crawlers that collect vast amounts of online content to train large language models (LLMs), giving publishers greater control over how their work is used.

The announcement follows growing criticism from media outlets and creators who claim their content is being used without consent or compensation. Unlike traditional search engine bots, AI crawlers can generate responses without crediting or linking to the original source, raising copyright and revenue concerns. Cloudflare's tool lets site owners detect and restrict these bots.

A "Pay Per Crawl" model is also being developed, which could allow sites to request payment for access. Publishers and content creators have welcomed this as a positive

step towards fairer value exchange, but experts warn that stronger legal protections, not just technical fixes, are still needed.

Learn more about Cloudflare's AI bot blocker

Amazon faces US class action over Alexa users' privacy

On 7 July 2025, a federal judge in Seattle ruled that tens of millions of Alexa users can proceed with a nationwide class-action lawsuit against Amazon for allegedly recording and storing private conversations without proper disclosure. The plaintiffs - users who registered Alexa devices – claim Amazon violated Washington State's consumer protection law and are seeking damages and an injunction to stop the recordings.

Amazon denies wrongdoing, stating their devices incorporate safeguards to ensure they only activate with 'wake' terms, such as 'hi Alexa'.

The case highlights privacy risks for Internet of Things (IoT) providers and other companies handling voice or audio data. Guidance from the Federal Trade Commission (FTC) states organisations should:

- Build security into IoT product design from the beginning
- Use recognised practices, such as encryption techniques and multifactor authentication (MFA)
- Implement effective authentication protocols and access controls
- Establish secure data management, including data minimisation practices and timely security reviews
- Actively monitor and address security risks
- Set clear security expectations for employees and provide regular training
- Be transparent with customers about security, using simple, clear, and direct communications

Read the FTC's IoT guidance

INTERNATIONAL

Singapore's IMDA launches new tools to support AI development

On 7 July 2025, Singapore's Infocomm Media Development Authority (IMDA) introduced three initiatives aimed at building a trusted ecosystem for the safe and responsible deployment of technologies.

Global AI Assurance Sandbox: Allows sector regulators to refine their governance frameworks and organisations to test real-world AI applications in a safe, controlled environment.

Privacy-enhancing Technologies (PET) Adoption Guide: Supports adoption of PETs by offering a use-case evaluation tool and implementation checklist, helping businesses integrate PETs safely.

Singapore Standard for Data Protection: Updates the Data Protection Trustmark (DPTM) by introducing enhanced requirements for third-party management and cross-

border transfers, and creating a streamlined certification process.

Learn more about the initiatives

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/Europe/Canada)**
- **Data Protection Support Officers (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