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.

Using AI for DSAR responses: What every organisation should know

Data Subject Access Requests (DSARs) are rising in volume and complexity, prompting many organisations to explore whether AI can help ease the burden. AI can speed up tasks like data discovery, redaction, and workflow management but it isn't an end-to-end solution. Relying on AI alone brings new challenges, ranging from accuracy issues to compliance risks.

Our latest blog examines the opportunities and risks of applying AI to DSAR response processes. We explain why human oversight remains essential and share practical guidance on adopting AI tools responsibly whilst staying compliant with data protection laws.

Read our blog

CANADA & UNITED STATES

Canadian regulators find TikTok's privacy protections inadequate

The Office of the Privacy Commissioner of Canada (OPC) and its provincial counterparts in Quebec, British Columbia, and Alberta have ruled TikTok's safeguards for young users fall short of Canadian privacy laws.

A joint investigation found that TikTok collected and used sensitive personal data from minors without a legitimate purpose, failed to obtain valid consent from adults for tracking,

profiling, and targeted advertising, and provided a privacy policy that lacked clarity and easy access to key details.

TikTok has agreed to improve age-verification methods and strengthen privacy communications to increase transparency around how user data is used.

The case highlights growing regulatory expectations of online platforms to deploy robust age-assurance measures, clearly explain data uses, and maintain strong safeguards to meet overlapping privacy obligations.

Read the investigation report

California finalises Regulations under CPPA

On 23 September 2025, California's Privacy Protection Agency (CPPA) announced that the Office of Administrative Law has approved new regulations under the California Consumer Privacy Act (CCPA). Designed to strengthen consumers' privacy, these rules will take effect from 1 January 2026, with phased compliance deadlines for various obligations.

In-scope organisations must:

- Complete cybersecurity audits and submit certifications between 2028 and 2030, depending on revenue thresholds
- Conduct mandatory risk assessments by 1 January 2026, with attestations and summaries due by 1 April 2028
- For entities using Automated Decision-Making Technology (ADMT) for significant decisions, comply with new requirements starting 1 January 2027

For organisations operating in or interacting with California, these regulations set a new bar for privacy requirements and underscore the critical importance of early preparation. The Regulations and supporting materials can be found on the **CPPA website**.

New research shows AI-powered phishing uses fake CAPTCHA

On 19 September, Trend Micro published **new research** exploring how cybercriminals are using AI tools to build and host convincing fake CAPTCHA pages. Attackers exploit free hosting services and familiar branding to make these CAPTCHAs appear credible, increasing the likelihood that users will click through. Automated scanners often stop at the CAPTCHA, allowing the attack to evade detection before redirecting users to malicious sites.

Trend Micro warns this approach is spreading rapidly as AI lowers the barrier to building realistic, scalable phishing infrastructure.

This trend illustrates how AI is reshaping social engineering. Organisations need a multi-layered defence that blends staff awareness, technical safeguards, and clear procedures. For practical steps on protecting your business, read our blog **AI social engineering attacks: Protect data and stay compliant**.

UNITED KINGDOM

Court of Appeal lowers the bar for non-material GDPR claims

The Court of Appeal has overturned a High Court decision on compensation for non-material damages under the UK GDPR. The case stemmed from a 2019 data breach at Equinity, where a system error sent more than 750 annual benefit statements containing sensitive personal data of Sussex Police officers to outdated addresses.

The High Court had struck out most of the 432 claims for lack of evidence that third parties accessed the data. The Court of Appeal ruled otherwise, confirming that:

- Sending personal data to the wrong address is ‘processing’ and can constitute an infringement
- There is no de minimis threshold for non-material damage
- Collective actions remain viable

The ruling highlights that even minor processing errors can potentially trigger data protection compensation claims, regardless of the level of perceived harm. Organisations should review their Risk Registers and, where relevant, Data Protection Impact Assessments (DPIAs) to ensure that relevant risks — especially those arising from routine operations — are properly identified and managed. Businesses should also audit key processes and review supplier contracts to ensure they understand and address the legal risks associated with non-compliance.

Read the ruling

EUROPEAN UNION

EDPS issues Opinion on EU-US government data transfers

On 17 September 2025, the European Data Protection Supervisor (EDPS) issued an Opinion on proposals for the sharing of information between EU Member State authorities and the United States for purposes such as border security and law enforcement. The

EDPS stressed that any such EU–US arrangement must include ‘comprehensive and effective safeguards’ to protect individuals’ privacy.

The EDPS warned that large-scale transfers, such as fingerprints or other identification data, pose serious privacy risks and must be strictly necessary and proportionate. Key recommendations include limiting the scope of shared data, excluding sensitive EU databases like migration or justice systems, and ensuring strong transparency, oversight, and judicial redress mechanisms in the United States.

For organisations handling cross-border data, the Opinion signals that any future EU–US law enforcement or security agreement will face a far higher bar for privacy protection than commercial transfers.

Read the Opinion

Italy becomes first Member State to enact AI legislation

On 17 September 2025, the Italian Senate approved Bill No. 1146 on artificial intelligence, creating a framework that aligns with the EU AI Act whilst addressing national priorities. The law promotes transparent and responsible AI use, balancing innovation with safeguards for fundamental rights, privacy, and social impact.

Key provisions:

- Personal data used in AI systems is processed lawfully, fairly, and transparently and remains compatible with the original collection purpose
- Users receive clear, simple information about data-processing risks
- Parental consent is obtained for minors under 14
- Sector-specific rules cover healthcare and scientific research
- New measures govern copyright for AI-assisted works and set liability for crimes involving AI, including financial offences and unauthorised distribution of AI-generated content

For organisations deploying AI in Italy, the law signals heightened expectations for data governance and transparency ahead of the EU-wide regime. Early steps, such as updating privacy notices, reviewing lawful bases for AI training data, and ensuring explainability, will help meet both Italian and forthcoming EU requirements.

Read Bill No. 1146

INTERNATIONAL

Kmart Australia's facial recognition use breaches Privacy Act

On 18 September 2025, Australia's Privacy Commissioner ruled that Kmart Australia Limited unlawfully collected customers' biometric data through a facial recognition system intended to deter refund fraud.

An investigation found Kmart neither notified shoppers nor obtained consent to capture their facial images, despite biometric data being classed as sensitive under the Privacy Act. The Commissioner rejected Kmart's claim of an exemption for preventing unlawful activity, noting the system captured every customer's facial image, offered limited benefit, and was disproportionate when less intrusive fraud-prevention methods were available.

Organisations should assess necessity and proportionality before using facial recognition or other biometric technologies, provide clear notice, and obtain valid consent where required. Read our **case study** to learn how a leading Live Facial Recognition (LFR) provider deployed the technology compliantly.

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)**
- **Accounts Assistant (United Kingdom)**

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

FOLLOW US ON LinkedIn