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.

Data Use and Access Act 2025: What UK Financial Services need to know

UK Financial Services firms are entering a new phase of regulated data sharing and access. The Data Use and Access Act (DUAA) 2025 introduces changes that affect how organisations participate in Open Finance, adopt digital verification services, and manage data governance in practice.

In this blog, we explore the changes that matter most and their impact on organisations. We outline where firms should focus now to prepare for phased implementation and evolving regulatory expectations.

Read our blog

CANADA & UNITED STATES

Ontario's IPC issues first administrative monetary penalty under PHIPA

In a decision relating to a health information breach, the Information and Privacy Commissioner of Ontario (IPC) imposed fines of $5,000 on an individual physician and $7,500 on a private clinic for unauthorised access and misuse of patients' personal health information. It marks the first time AMPs have been applied under the Personal Health Information Protection Act (PHIPA) since these powers came into force in 2020.

The penalties reflect growing regulatory scrutiny of privacy governance in healthcare. The decision underscores the need for clear access controls, documented privacy practices, and demonstrable compliance, particularly where sensitive health data is involved.

Read the IPC decision

California data breach notification deadlines now in force

Senate Bill 446 introduced fixed timelines for organisations handling personal data of California residents. From 1 January 2026, businesses must notify affected individuals within 30 calendar days of discovering or being notified of a data breach involving personal information. Where a breach affects more than 500 California residents, organisations must also submit a sample copy of the notification to the California Attorney General within 15 calendar days of issuing notices to individuals.

Previously, California's breach notification law required notice *'without unreasonable delay'* but did not set a specific deadline. The introduction of fixed timelines reflects a wider move towards clearer breach notification expectations, reinforcing the need for well-rehearsed incident response processes and up-to-date notification templates.

Read our blog for tips on effective data breach response.

Texas AG files lawsuit over smart TV data collection

The Texas Attorney General has filed legal action against Sony, Samsung, LG, Hisense, and TCL, alleging they unlawfully collected and monetised consumers' viewing data through Automated Content Recognition (ACR) technology. According to the Attorney General, ACR software embedded in smart TVs:

- Captured screenshots of on-screen content at frequent intervals
- Monitored viewing activity in real time
- Transmitted information back to manufacturers without users' knowledge or meaningful consent

The data was then allegedly sold to support targeted advertising across platforms.
The Attorney General has since secured a temporary restraining order against Hisense, preventing the company from collecting, using, selling, sharing, or transferring ACR data about Texans while the case proceeds.

The action highlights growing regulatory scrutiny of 'always-on' consumer technologies and reinforces the need for clear transparency, valid consent, and robust governance where behavioural data is collected at scale.

Find out more

UNITED KINGDOM

NHS healthcare tech provider confirms data breach

UK-based DXS International, used by around 2,000 GP practices, discovered the breach on 14 December. The company immediately engaged external specialists to investigate the nature and scope of the incident, but it is not yet clear if patient data was compromised. A ransomware group known as DevMan has taken credit for the attack, claiming to have exfiltrated about 300 GB of data.

The breach underscores ongoing security challenges across NHS technology suppliers and the potential damage to patient trust when sensitive data is exposed. Strong data protection practices are critical to maintaining confidence in healthcare services.

Learn how data protection builds customer trust and loyalty

EUROPEAN UNION

Austrian court ruling reinforces DSAR response obligations

On 18 December 2025, Austria's Supreme Court (OGH) ruled that Meta must disclose all personal data in response to a valid Data Subject Access Request (DSAR), including details of data sources, purposes, and recipients. The court rejected Meta's arguments that technical complexity, proprietary systems, or reliance on automated access tools could justify restricting DSAR disclosures.

The decision reinforces the strength of access rights under the General Data Protection Regulation (GDPR) and sends a clear signal to organisations operating in the EU: DSAR compliance cannot be partial, selective, or shaped around internal convenience. For organisations handling large volumes of personal data, the ruling highlights the need for robust data mapping, transparent processing records, and DSAR processes that work in practice.

Watch our webinar to learn key strategies for effective DSAR response.

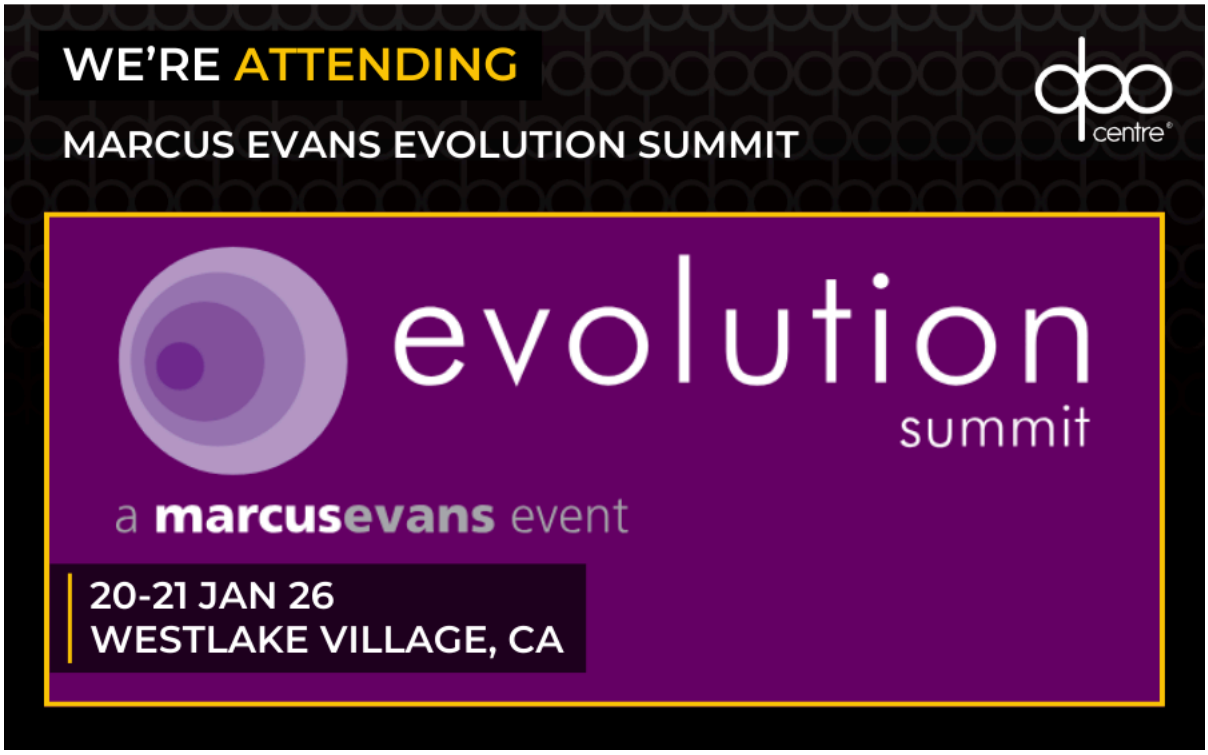
CJEU rules body-worn camera data is collected directly

The Court of Justice of the European Union (CJEU) has ruled that personal data captured through body-worn cameras is collected directly from the data subject, resolving ongoing uncertainty over whether such footage falls under Articles 13 or 14 of the General Data Protection Regulation (GDPR). The Court confirmed that Article 13 GDPR applies, meaning individuals must be informed at the point their data is collected.

The CJEU also confirmed that this obligation can be met through a layered transparency approach, for example, through clear on-site signage supported by easily accessible additional information, such as a full privacy notice.

Paul Collier, Head of Data Protection at The DPO Centre, said: *'The recent CJEU ruling makes it clear: when data is collected directly from individuals using devices such as Body Worn Video (BWV), transparency isn't optional; it's non-negotiable. Organisations therefore must provide clear, transparent and accessible privacy information at the point of collection, whether through just-in-time notices, audible alerts that recording is taking place, or innovative solutions like QR codes.'*

Learn how to write a clear and compliant Privacy Notice



INTERNATIONAL

Hong Kong PCPD publishes toolkit on AI-generated deepfakes

On 17 December 2025, the Office of the Privacy Commissioner for Personal Data (PCPD) published *Abuse of AI Deepfakes*, a toolkit designed to help schools and parents understand and manage the privacy risks associated with AI-generated synthetic media.

The guide:

- Provides practical insights into how personal data may be processed in the context of generative AI
- Identifies key risk areas, such as consent, transparency, and accuracy
- Sets out risk mitigation strategies for compliance with the Personal Data (Privacy) Ordinance (PDPO)

The guidance signals increasing regulatory attention on the governance of synthetic media. Organisations using or encountering AI-generated content are expected to take a proactive approach to oversight, ensuring privacy considerations are embedded into decision-making, controls, and organisational accountability.

Read the toolkit

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)**
- **Chief Revenue Officer (United Kingdom)**

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

FOLLOW US ON LinkedIn