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 protection & AI governance 2025-2026

Data protection and AI legislation has continued to evolve this year, often in diverging directions. In highly regulated sectors, such as Healthcare and Financial Services, these changes have had a significant impact. For multi-national organisations, managing compliance across borders is an increasing challenge.

In our final blog of 2025, we look back at the year's major privacy and AI developments. We explain what the changes might mean for organisations operating in the UK, EU, Canada, and the US, and highlight the areas organisations should address as we step into 2026.

Read our blog

UNITED KINGDOM

ICO fines password manager provider £1.2M following data breach

The breach, which occurred at LastPass in 2022, exposed the personal information of up to 1.6 million UK users. The Information Commissioner's Office (ICO) found that insufficient technical and organisational measures allowed a hacker to gain unauthorised access to a backup database, compromising customer names, email addresses, and phone numbers.

The ICO emphasised the need for security policies to clearly address data breach risks, with access to high-risk systems and data strictly limited to defined user groups.

Organisations should ensure robust access controls, risk-based security policies, and regular testing of backup environments.

Read the ICO's guidance on data security

Court examines re-identification risk following data breach

On 4 December 2025, the UK Court of Appeal heard the ICO v DSG Retail case following a cyber incident in which hackers accessed DSG's systems.

The breach involved payment card data from around 5.6 million cards, including the 16-digit card number and expiry date. DSG reported the incident, but the Information Commissioner's Office (ICO) concluded that the retailer had failed to implement appropriate safeguards and issued a £500,000 fine in 2020 — the maximum penalty available under the Data Protection Act 1998.

DSG disputes the ICO's position, arguing that the compromised data was not personal data in the hands of the hackers, as it was not directly identifiable. The ICO argues that the data should be treated as pseudonymised data, as it could have been re-identified if combined with other information, either held by DSG or obtained elsewhere, creating a risk of fraud.

The court considered EU case law on identifiability, including the recent EDPS v SRB case, which provided fresh clarification on the status of pseudonymised data under the EU General Data Protection Regulation (GDPR).

Judgement has been reserved, but the forthcoming decision may shape how organisations assess identifiability and security obligations following data breaches.

Read our blog to learn what the EDPS v SRB ruling means for organisations.

EUROPEAN UNION

CNIL fines American Express €1.5M for cookie compliance failures

France's data protection authority found that the company breached Article 82 of the French Data Protection Act by:

- Placing trackers without obtaining user consent
- Continuing to deposit trackers despite users refusing consent
- Reading trackers even after consent was withdrawn

The decision reinforces that cookie compliance remains a regulatory priority. Organisations must ensure that consent mechanisms are robust, that trackers are blocked until consent is obtained, and that any withdrawal of consent is respected in real time.

Read the CNIL's cookie recommendation

European Commission launches Data Act Legal Helpdesk

The helpdesk provides direct support to organisations and public authorities on how to apply the EU Data Act, offering practical guidance on the Regulation's requirements, rights, and obligations. It is intended to support all stakeholders navigating the Data Act's implementation, particularly SMEs.

The Commission has also confirmed that further support is planned, including guidelines on reasonable compensation and additional guidance on key definitions under the Regulation.

As the Data Act moves towards application, organisations should make use of this support to clarify obligations and prepare internal processes for compliance.

Access the Legal Helpdesk

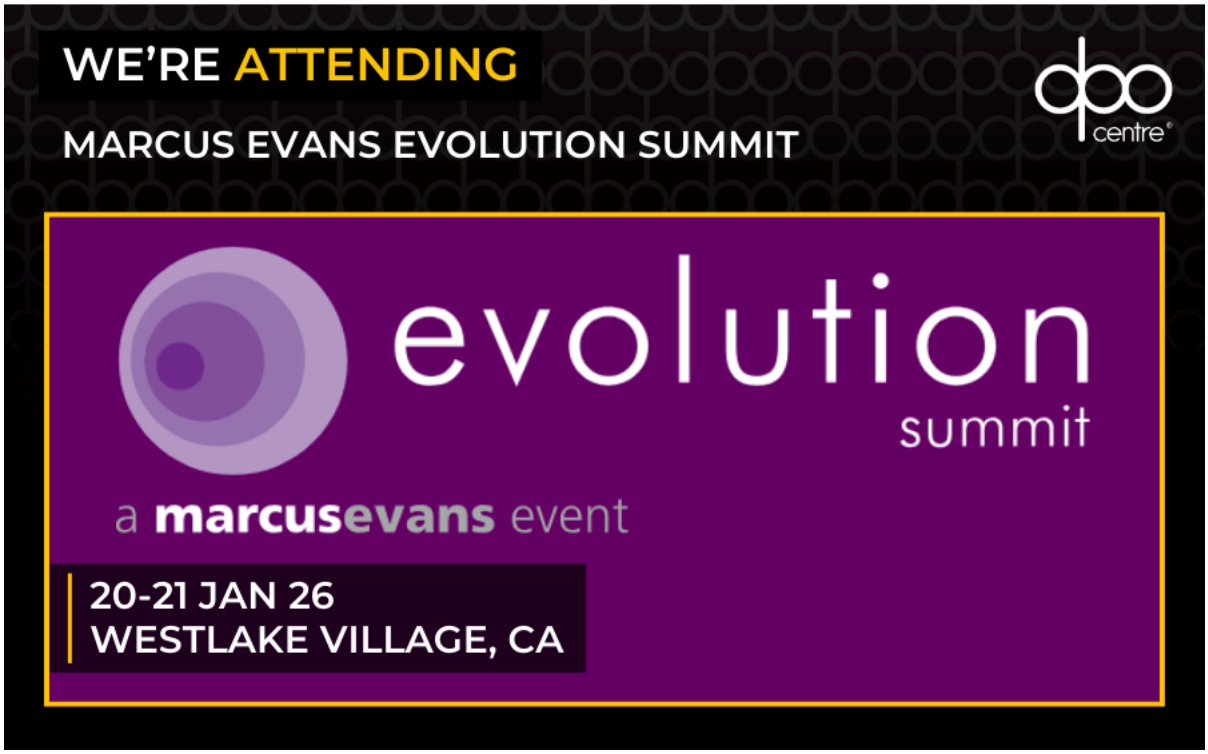
Dutch DPA to check data protection at Healthcare providers

The Dutch data protection authority, Autoriteit Persoonsgegevens (AP), has announced it will begin spot-checks on healthcare providers to assess how patient and client data is handled.

The move follows more than 6,800 data breach reports from the Healthcare sector in 2024 — the largest share of breach notifications received by the AP last year, according to its Data Breach Report 2024.

The AP has emphasised that Healthcare organisations must ensure personal data is properly secured against hackers and data breaches, with appropriate technical and organisational measures in place.

Read the AP's Health guidance for more information on applicable rules and compliance expectations.



CANADA & UNITED STATES

US President signs executive order to block state AI regulation

On 11 December 2025, US President Donald Trump signed an executive order aimed at preventing US states from enforcing their own AI laws, signalling a move to centralise AI governance at the federal level.

The order is intended to avoid a fragmented, state-by-state approach to AI regulation, which the administration argues could hinder innovation and weaken US competitiveness. By limiting state intervention, the White House aims to support faster AI development and deployment across the US.

But critics argue the move leaves a regulatory gap. In the absence of comprehensive federal AI safeguards, state-level rules have been used to address issues such as algorithmic bias, transparency, and consumer protection.

The order highlights growing tension in the US between innovation-led AI policy and demands for accountability. For organisations operating across multiple states, it may reduce short-term compliance complexity, but longer-term uncertainty remains until a federal AI framework is established.

Read the executive order

Canada and EU sign Memorandum of Understanding on AI

On 8 December 2025, Canada and the European Union formalised closer cooperation on AI standards, regulation, skills development, and adoption.

Under the MoU, both partners commit to:

- Sharing best practices to accelerate AI adoption in strategic sectors such as Healthcare, Science, and Public Services
- Working together on large-scale AI infrastructure
- Addressing barriers faced by SMEs, including challenges around commercialisation and deployment
- Supporting the development of advanced AI models for the public good, including use cases such as climate change and extreme weather monitoring
- Establishing a structured dialogue on data spaces, recognising their growing importance in the development, training and deployment of large AI models

For organisations with EU–Canada operations, the agreement signals a move towards greater interoperability in AI governance, infrastructure, and standards.

Learn more about the MoU on AI

INTERNATIONAL

eCommerce breach exposes personal data of almost 34M customers

South Korean eCommerce giant, Coupang, has disclosed a significant data breach affecting the personal information of approximately 33.7 million customers. The exposed data included names, email addresses, phone numbers and shipping addresses. Payment details and login credentials were reportedly not compromised.

Coupang identified the unauthorised access on 18 November 2025, but subsequent investigations suggest the breach may have begun as early as June 2025 via an overseas server. The scale of the incident, combined with the length of time it went undetected, raises concerns around access controls, insider threat management, and continuous security monitoring.

Organisations should review their security visibility, incident detection capabilities, and response procedures to minimise the time between compromise and discovery.

Customers have been urged to remain alert to scams and impersonation attempts using their contact details. **Read our blog** to learn how to defend your organisation against social engineering attacks.

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, 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