the dpia

GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE



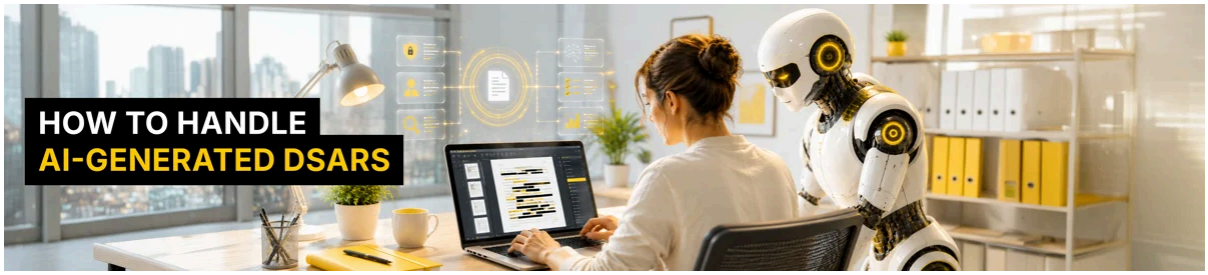
The DPIA is an assessment of the impact of the most significant and important-to-know data protection issues from around the globe. It's not the full story, just a quick 3-minute read, collated and condensed to keep you updated with the latest news in our ever-evolving industry.

How to handle AI-generated DSARs

Generative AI is making it easier for individuals to create lengthy and highly detailed Data Subject Access Requests (DSARs), potentially increasing the time and resources needed to respond. However, the use of AI does not change an individual's right of access or automatically justify limiting or refusing a request.

Our latest blog explains how organisations can manage complex AI-generated DSARs, when they can legally clarify, extend or refuse a request, and how to strengthen their processes to ensure responses remain reasonable, proportionate and defensible.

Read our blog



UNITED STATES & CANADA

California introduces new protection for workplace AI and surveillance

On 30 September 2026, the Governor of California signed new legislation introducing safeguards for employees affected by AI-driven decisions and workplace monitoring.

The measures include:

- SB 947: Prohibits employers from relying solely on automated systems when making disciplinary or dismissal decisions
- SB 951: Requires employers to disclose when certain workforce reductions are caused by AI

- AB 1331 and AB 1883: Introduce restrictions on workplace surveillance, including monitoring in bathrooms

The legislation highlights growing expectations for organisations to maintain meaningful human oversight of AI-supported employment decisions and ensure workplace monitoring is appropriately controlled.

Watch our webinar to explore the data protection considerations surrounding employee monitoring.

Canada publishes fact sheet on proposed Safe Social Media Act

The Act, known as Bill C-34, would introduce new requirements for social media platforms and other regulated services.

Presented as a Q&A, the fact sheet helps organisations understand the reasoning behind the Bill, who and what would fall within scope, its intersection with AI, and how the proposed regime would be enforced. It also provides an early indication of the privacy requirements organisations may need to prepare for, particularly when designing age assurance methods.

Organisations likely to fall within scope should familiarise themselves with the proposals and consider what changes may be needed to their age assurance, data handling, and privacy processes if the Bill becomes law.

Read the fact sheet

Connecticut Data Privacy Act amendments take effect

Amendments to the Connecticut Data Privacy Act (CTDPA) came into effect on 1 October 2026, introducing stronger protections for consumers and new requirements for organisations processing personal data.

Key changes include:

- Restrictions on the use of facial recognition technology, including transparency requirements
- A prohibition on the sale of consumers' precise geolocation data
- New restrictions and disclosure requirements for surveillance pricing, where personal data is used to determine individual prices
- Additional protections for genetic data and new regulatory requirements for data brokers

Organisations operating in Connecticut should review their data collection, sharing and transparency practices to ensure compliance with the applicable requirements.

Read the Connecticut Attorney General's guidance



*The DPO Centre brings together specialists from across the Axiom GRC group for **five expert-led webinars**. Each session focuses on a key AI challenge creating new risks for organisations. Sign up for one, or join us for all five.*

UNITED KINGDOM

NHS expands guidance on unlawful access to health records

Following a series of cases involving inappropriate access to patient information, NHS England has updated its guidance on how organisations should prevent, monitor, and investigate unlawful access.

It recommends:

- Risk-based audits of access to electronic patient records
- Technical controls such as role-based access and Multi-Factor Authentication (MFA)
- Live monitoring and flagging of access to an employee's own records, or those of colleagues, relatives and high-profile individuals

Teams should treat suspected inappropriate access as a potential personal data breach and involve their DPO early to assess whether ICO reporting or notification to affected individuals is necessary.

Read the guidance

EUROPEAN UNION

Italian DPA fines health data company €7M for anonymisation failures

An investigation by the Data Protection Authority (GPDP) in April 2025 found that IQVIA's dataset, which covered around 1 million patients from 800 GPs, was not anonymous. It also reported issues with its data processing practices, including no appropriate lawful basis, lack of retention policies, and the absence of a DPIA.

The case serves as a reminder that anonymisation does not simply mean removing obvious identifiers. Organisations must consider whether individuals could still be singled out or reidentified when coded data is combined with other information in the dataset.

Read our blog to learn about the challenges of anonymisation and effective techniques to reduce risk.

DPC orders Children's Health Ireland to finalise DPIAs

A 2025 investigation by Ireland's Data Protection Commission (DPC) found that Children's Health Ireland (CHI) failed to ensure the appropriate security and confidentiality of children's health records at its Tallaght facility. The investigation identified issues with the management of paper records and confidential waste containing sensitive and special category data.

The DPO has reprimanded CHI and ordered it to finalise DPIAs covering healthcare records and confidential waste management. CHI must also fully implement the technical and organisational measures identifies through the assessments.

Read the DPO Centre guide to DPIAs



INTERNATIONAL

Singapore publishes implementation guidance for Health Information Act

The Health Information Act (HIA) introduces mandatory health information sharing through the National Electronic Health Record (NEHR), alongside new cyber and data security requirements.

Implementation will be phased across healthcare providers, with key deadlines including:

- September 2027: GPs, private hospitals and certain diagnostic service
- September 2028: Specialist outpatient services and other healthcare providers
- March 2030: Dental clinics, assisted reproduction centres and retail pharmacies

Organisations within scope should review their existing systems, data-sharing arrangements, and security measures to identify what changes may be needed ahead of their respective deadlines.

Explore the implementation guidance



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 Officer - Life Sciences (United Kingdom)**
- **Data Protection Officer (Poland)**
- **Data Protection Officer - Life Sciences (Poland)**
- **Data Protection Coordinator - Life Sciences (Poland)**

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

FOLLOW US ON LinkedIn

Copyright © 2026 The DPO Centre, All rights reserved.

You have been sent this newsletter under legitimate interest, for more information please read our Privacy Notice
The DPO Centre is a limited company registered in England and Wales (Company Number: 10874595)

The DPO Centre Group
London | Amsterdam | Toronto | Dublin

Unsubscribe Manage Preferences