



The DPOIA 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: Why low-risk data processing can still create risk

GDPR compliance gaps don't always stem from obviously high-risk processing activities. Sometimes they arise from routine systems and processes that are rarely challenged or reassessed. Activities such as email, internal collaboration tools, customer interactions, and data aggregation can create elevated risks depending on how information is accessed, combined, retained, and used in practice.

In our latest blog, we explore how assumptions around 'low-risk' processing can lead to overlooked compliance gaps and explain how organisations can take a more effective risk-based approach to identifying and managing hidden GDPR risks.

[Read our blog](#)



CANADA & UNITED STATES

Gartner reports sharp rise in US privacy enforcement fines

The research firm estimates that US states issued \$3.425 billion in privacy-related fines during 2025, exceeding the total value of fines issued over the previous five years combined. The trend is expected to accelerate through 2028 as state privacy laws continue to expand and mature.

According to Gartner, most enforcement actions relate to shortcomings in privacy user experience, including issues linked to subject rights, consent mechanisms, and privacy

notices. With regulators placing increasing focus on automated decision-making technologies and AI governance, the findings highlight the importance of ensuring privacy controls remain clear, accessible, and appropriately updated as AI adoption evolves.

[Read our blog on updating privacy notices for AI](#)

Canadian investigation highlights risks of unauthorised access breaches

The Office of the Privacy Commissioner of Canada (OPC) has highlighted more than 42,000 individual privacy breaches at the Canada Revenue Agency (CRA) since 2020, with affected individuals experiencing financial loss and other significant impacts.

The report noted that many incidents involved bad actors gaining unauthorised access to personal information. The findings highlight the growing risks posed by phishing, credential theft, and social engineering attacks, particularly as threat actors increasingly use AI to scale and automate attacks.

[Read our blog](#) to learn how to defend your organisation.

FTC begins enforcing TAKE IT DOWN Act requirements

The US Federal Trade Commission (FTC) has begun enforcing the TAKE IT DOWN Act (TIDA), which introduces new obligations for online platforms handling intimate images shared without consent.

From 19 May 2026, covered platforms must provide a clear process for users to submit removal requests, remove reported content and known duplicates, and complete the removal process within 48 hours of receiving a valid request.

To assist businesses in understanding their obligations, the FTC has produced guidance clarifying which organisations fall within scope and how the new requirements should be applied in practice.

[Read the FTC business guidance](#)

PRIVACY PUZZLE WEBINAR

Privacy Puzzle
GLOBAL WEBINAR SERIES
16 JUN 2026

EU & UK CLINICAL TRIALS: Are you clear on your data protection and legal representation requirements?

dpo centre

Katarzyna Wieckowska
dpo centre

Rik Mannix
dpo centre

Wafa Bouaziz
DLRC

Kadi Kuuskmae-Perry
DLRC

REGISTER NOW

UNITED KINGDOM

ICO shares guidance on AI-driven data breach risks

On 14 May 2026, the Information Commissioners Office (ICO) published 5 steps to help organisations protect themselves against AI-powered cyber threats.

The ICO recommends organisations:

- Understand potential threats, highlighting seven key AI-powered cyber risks
- Layer defences through technical controls, patching, and secure configurations
- Restrict access points using measures such as multi-factor authentication (MFA), strong password policies, and least privilege access
- Improve detection, monitoring, and incident response processes
- Implement appropriate technical and organisational measures to protect personal data

[Read the ICO guidance](#)

EUROPEAN UNION

European Commission publishes draft guidance on high-risk AI systems

Published on 19 May 2026, [the guidance](#) aims to help providers, deployers, and competent market surveillance authorities determine whether an AI system should be classified as high-risk under the EU AI Act. It explains how key provisions of the Act should be interpreted in practice and contains use cases to demonstrate how classification decisions may apply across different sectors.

The Commission invites AI stakeholders, including public authorities and research institutions, to provide their feedback on the draft guidelines by 23 June 2026.

[Read our article](#) for advice from our AI Sector Lead on what organisations should do next.

CNIL reports record data breach notifications in 2025

The French data protection authority (CNIL) has reported a record 6,167 data breach notifications in its 2025 annual report, with hacking responsible for around half of all reported incidents.

The findings reflect the continued growth in cyber-related breaches and increasing pressure on organisations to strengthen technical and organisational security measures. CNIL noted that ransomware, credential theft, and phishing remain significant causes of compromise.

The report highlights the importance of maintaining effective security controls, incident response processes, and staff awareness measures to reduce the risk of breaches.

[Read the CNIL annual report](#)



INTERNATIONAL

China publishes ethics and safety guidelines for AI applications

On 19 May 2026, China's National Cybersecurity Standardization Technical Committee (TC260) published the Ethics-Safety Guidelines for Artificial Intelligence Applications 1.0.

The guidelines establish nine core principles for the development and deployment of AI applications, alongside practical requirements for developers relating to areas such as

transparency, accountability, and incident traceability.

[Read the guidelines](#)



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 (The Netherlands)**
- **Data Protection Officers (Poland)**
- **Data Protection Officers - Life Sciences (United Kingdom)**
- **Data Protection Coordinator - Life Sciences (Poland)**
- **Data Protection Officers - Life Sciences (Poland)**
- **Senior Commercial Executive - Life Sciences (United Kingdom)**
- **Senior HR Advisor - maternity cover (United Kingdom)**

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](#)