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.

AI Impact Assessments: What are they and why do you need one?

AI tools are quickly becoming embedded into everyday organisational practices. But these opportunities bring increased risks, such as bias, discrimination, lack of transparency, and potential harm to individuals. An AI Impact Assessment (AIIA) helps organisations identify these risks early, demonstrate accountability, and build trust in their AI systems.

In our latest blog, we explain what an AIIA is, when it's required, and how to conduct one effectively. Outlining its role under the General Data Protection Regulation (GDPR) and EU AI Act, we share practical steps for integrating AIIAs into the AI lifecycle and answer common questions to help organisations adopt AI responsibly and with confidence.

Read our blog

UNITED KINGDOM

ICO seeks public input on new data protection complaints process

On 22 August 2025, the UK Information Commissioner's Office (ICO) launched a consultation on proposed changes to how it handles data protection complaints. The move comes in response to an 8% increase in complaint volumes, from 39,721 in 2023/24 to 42,881 in 2024/25, and forecasts that numbers could climb as high as 55,000.

Under the incoming Data Use and Access Act (DUAA), organisations will be required to have their own data protection complaints processes by June 2026. The ICO's draft framework proposes new criteria to assess which complaints warrant ICO intervention, aiming to prioritise cases where the regulator's impact will be greatest. The consultation also suggests enhanced reporting to allow sector-wide trend analysis and earlier detection of systemic issues.

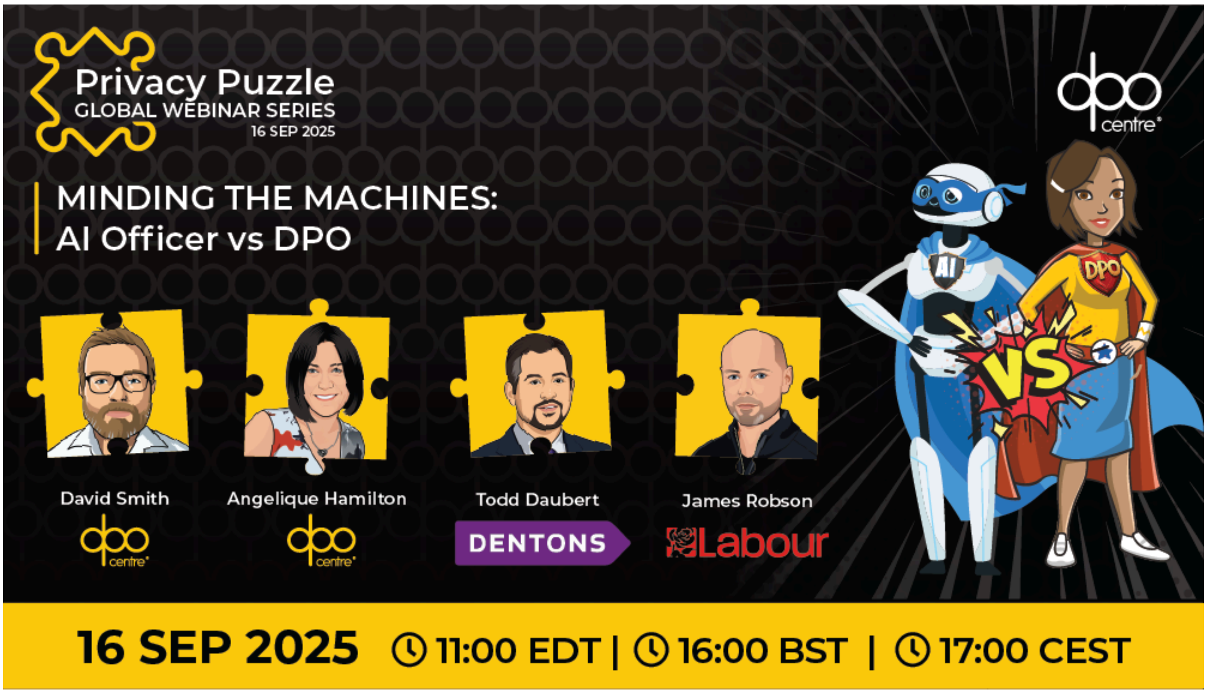
Learn more about the consultation, which is open until 31 October 2025.

UK MoD admits to 49 Afghan data breaches

The UK Ministry of Defence (MoD) has admitted to 49 data breaches involving Afghan relocation applicants between 2021 and 2025. The breaches first came to light after a 2022 spreadsheet error exposed thousands of applicants' details, but a super-injunction prevented disclosure for nearly two years while a covert relocation programme took place.

The revelations highlight serious weaknesses in data handling and accountability, particularly when processing sensitive information about vulnerable individuals. The case underscores the need for robust security measures, transparent incident reporting, and data governance frameworks.

Learn more about the breaches



EUROPEAN UNION

Austrian court rules DerStandard's 'consent or pay' model unlawful

Austria's Federal Administrative Court (BVwG) has upheld a decision by the Austrian Data Protection Authority (DSB) concerning a news outlet's use of a 'consent or pay' model. The court confirmed that newspaper DerStandard breached the General Data Protection Regulation (GDPR) by tying access to content to blanket consent. It ruled that users must be able to selectively consent or object to individual processing purposes, rather than only accepting or rejecting all processing globally.

On appeal, the publisher argued that granular consent was not feasible within its business model, but the court confirmed that GDPR requires specific, purpose-based consent.

This decision follows wider EU scrutiny of ‘consent or pay’ models. In Opinion 08/2024, the European Data Protection Board (EDPB) stressed that consent must be freely given and that users should be offered a genuine choice beyond either paying or agreeing to behavioural tracking.

Denmark appoints DPA to oversee AI Regulation prohibitions

On 2 August 2025, the Danish Data Protection Agency (Datatilsynet) was appointed as the supervisory authority for selected provisions of the EU AI Regulation. Its role will focus on ensuring compliance with the Regulation’s bans on certain high-risk AI practices set out in Article 5.

Specifically, Datatilsynet will oversee the prohibitions on:

- AI systems that carry out risk assessments of individuals to predict the likelihood of committing criminal offences, based solely on profiling or personal characteristics
- AI systems used for biometric categorisation to infer sensitive attributes

Although the right to complain and the obligation to report serious AI incidents will not take effect until 2 August 2026, Datatilsynet can already respond to enquiries and open investigations on its own initiative.

For a wider overview of prohibited AI practices, read our blog on compliance with the AI Act.

Italy’s cyber agency issues 20 recommendations on CCTV and IoT risks

Italy’s National Cybersecurity Agency (ACN) has published 20 recommendations for organisations to improve the security of video surveillance systems and Internet of Things (IoT) devices. The guidance follows growing concerns that poorly configured cameras and connected devices can expose sensitive personal data, create entry points for attackers, and undermine public trust.

The recommendations include:

- Conducting continual staff training on IT security
- Setting strong, unique passwords and using multi-factor authentication (MFA)
- Applying timely security updates and patches
- Enforcing role-based access controls
- Continual monitoring and testing of systems and response procedures

Organisations using CCTV or IoT devices are encouraged to adopt the ACN’s recommendations to reduce breach risks and strengthen accountability.

Read the recommendations

CANADA & UNITED STATES

Colorado's AI Act amendment sets new duties for developers and deployers

On 26 August 2025, Colorado passed a comprehensive amendment to its Artificial Intelligence Act (SB 24-205), outlining new obligations for creators and users of high-risk AI systems.

Developers must:

- Safeguard against algorithmic discrimination
- Provide documentation for impact assessments
- Disclose system risks to the state Attorney General
- Publish transparency statements about their high-risk systems

Deployers must:

- Adopt comprehensive risk management programmes
- Conduct annual impact assessments
- Notify the Attorney General of any discrimination discovered within 90 days

Originally set to take effect in February 2026, implementation has now been postponed to 30 June 2026. Developers and deployers should now assess whether their AI practices meet these requirements.

Read the Act

OCR fines accounting firm $175K for HIPAA risk analysis failures

On 18 August 2025, the US Department of Health and Human Services' Office for Civil Rights (OCR) announced a $175,000 settlement with New York-based business associate

BST & Co. The settlement resolves allegations that BST failed to conduct a thorough risk analysis under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, following a ransomware incident in December 2019 that compromised protected health information of up to 170,000 individuals.

Under the HIPAA Security Rule, organisations must conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). This analysis should be documented, kept up to date, and used as the basis for putting security safeguards in place.

Guidance on risk analysis

INTERNATIONAL

The Bahamas publishes draft Data Protection Bill for consultation

On 21 August 2025, The Bahamas' Office of the Data Protection Commissioner published the draft Data Protection Bill 2025 for public consultation. The Bill aims to modernise the country's privacy framework, replacing the Data Protection (Privacy of Personal Information) Act 2003.

Reflecting GDPR principles, the Bill proposes:

- Enhanced rights for data subjects
- Greater transparency, accountability, and security obligations for controllers and processors
- Requirements around data transfers, appointment of Data Protection Officers (DPOs), automated processing, breach notification, and Data Protection Impact Assessments (DPIAs)

Notably, the Bill also includes provisions designed to address emerging industries and technologies, such as Fintech, eCommerce, AI, and biometrics. Its scope extends to overseas organisations, requiring controllers or processors not established in The Bahamas to nominate a local representative.

The consultation is open to the public, businesses, civil society, and industry stakeholders, with a public forum scheduled for early September.

Read the draft Bill

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 Support Officers (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

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 | New York | Toronto | Dublin

Unsubscribe Manage Preferences