the dpia

GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE



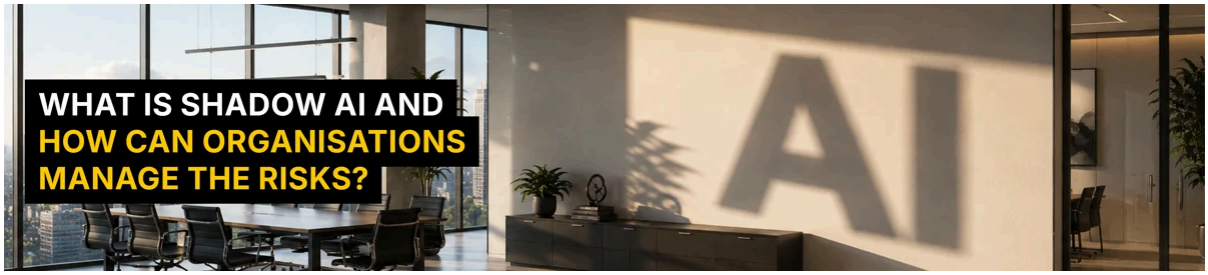
**The DPIA is an assessment of the impact of the most significant and important-to-know data protection issues from around the globe. It's not the full story, just a quick 3-minute read, collated and condensed to keep you updated with the latest news in our ever-evolving industry.**

# What is shadow AI and how can organisations manage the risks?

Shadow AI goes beyond employees using unapproved tools. It can reveal gaps in an organisation's visibility and governance, leaving businesses unaware of how AI is being used and the risks it may create.

Our latest blog explores why shadow AI develops, the data protection risks involved, and how organisations can strengthen their AI governance whilst supporting legitimate use.

**Read our blog**




## UNITED KINGDOM

# ICO reprimands two organisations over weak password security

An investigation by the Information Commission's Office (ICO) found that a 2024 ransomware attack on Ogi Networks Limited and Data Cymru compromised the personal data of 3,300 people, most of whom were children.

The attack exploited a test account that had existed for over 12 years and was protected by the password 'Password1'.

The ICO identified failures in account management, security monitoring and the allocation of responsibilities between the organisations. It reminds businesses to:

- Use strong passwords
- Implement Multi-Factor Authentication (MFA) for remote access
- Regularly review and remove unnecessary accounts
- Clearly define cybersecurity responsibilities when outsourcing IT services

Read our blog for practical guidance on effective password management.

## NHS England highlights cybersecurity and AI governance risks

NHS England has raised its technology and innovation risk score from 8 to 12, citing delays to major digital programmes such as the Federated Data Platform and single patient record. The Board called for a more coordinated, risk-based approach to AI governance, with appropriate safeguards throughout the AI lifecycle.

Cybersecurity remains its highest-rated risk at 25, with a high number of organisations receiving a 'Standards Not Met' assessment under the Data Security and Protection Toolkit (DSPT).

These findings highlight the need to assess whether existing security controls can support increasingly complex digital systems. Regularly reviewing DSPT compliance, addressing identified weaknesses, and ensuring appropriate oversight of new technologies can help protect patient information and maintain service continuity.

Read our blog for the latest DSPT submission requirements and common mistakes to avoid.




*The DPO Centre brought together specialists from across the Axiom GRC group for **five expert-led webinars**. Each session focused on a key AI challenge creating new risks for organisations. Watch all five webinars on demand.*

EUROPEAN UNION

# EU Council agrees position on Digital Omnibus proposals

The Digital Omnibus aims to simplify aspects of EU data protection and cybersecurity legislation. The proposed changes could affect how organisations handle Data Subject Access Requests (DSARs), report personal data breaches and manage cookie consent, alongside other GDPR obligations.

Whilst the proposals aim to reduce compliance burdens, they could also widen the differences between UK and EU data protection requirements. Organisations operating across both jurisdictions may therefore need to adapt their compliance processes.

Read our latest article for a breakdown of the proposed changes and insight on what they could mean for businesses from Paul Collier, Head of DPOs at the DPO Centre.

# Denmark population register breach exposes 8.8 million records

Denmark's Central Person Register (CPR) has suffered a major data breach affecting approximately 8.8 million registered individuals. The exposed information includes names, addresses, and CPR identification numbers of current residents, people who have moved abroad and those who are deceased.

The incident involved unauthorised individuals exploiting a private company's legitimate access to the register, highlighting the risks associated with third-party access to personal data. Even where access is authorised, organisations must ensure appropriate safeguards are in place, including restricted permissions, monitoring for unusual activity and regular access reviews. Clear incident response procedures are also essential for identifying, containing, and assessing potential breaches.

Read our blog for five tips on effective data breach management.

# Dutch regulator publishes draft guidance on switching cloud providers

The Netherlands Authority for Consumers and Markets (ACM) has published draft guidance clarifying the rights and obligations of cloud providers and customers under the EU Data Act.

The guidance covers four key areas:

- Providers must support customers switching services or using multiple providers without unnecessary obstacles
- Customers must receive clear information about switching arrangements, costs and timelines
- Providers must support data portability and interoperability, including through free APIs
- Providers must protect non-personal data against unlawful access or transfer by non-EU governments

For organisations using cloud services, the guidance offers an opportunity to review provider contracts, data portability arrangements, and exit strategies to ensure they can switch services without unnecessary disruption.

Read the ACM's draft guidance which is open for consultation until 6 November 2026.




## UNITED STATES & CANADA

# Meta ordered to pay $25B over misleading data privacy claims

A New Mexico court has ordered Meta to pay $25 billion in civil penalties for violating the state's consumer protection laws. A jury found that Facebook misled consumers about how their personal data was processed, including claims about users' control over their information, third-party access to personal data, and Meta's response to data misuse.

The ruling highlights the importance of ensuring privacy notices and other public-facing communications accurately reflect how personal data is handled in practice. Organisations should regularly review their privacy statements, third-party data-sharing arrangements, and internal controls to ensure they can substantiate the assurances they give individuals.

Read our blog for guidance on creating clear and compliant privacy notices.

# OPC of Canada updates guidance on recording customer calls

The updates focus on the collection of voiceprints, which are considered sensitive biometric information, and the need for meaningful consent. Whilst implied consent may be sufficient for routine call recordings, express consent may be required when collecting voiceprints or other sensitive information for purposes such as identity verification.

Organisations subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) must comply regardless of who initiates the call. They must also ensure that outsourced call centres and other third-party providers meet these requirements.

**Read the updated guidance**

## INTERNATIONAL

# Thailand's Cloud Security Standard comes into effect

In force from 10 September 2026, it introduces cybersecurity assessment and assurance requirements for cloud service providers and certain organisations using cloud services.

The standard requires affected organisations to:

- Assess the potential impact of their cloud systems
- Identify applicable security controls
- Maintain evidence of compliance

Depending on their role and the system's impact level, organisations may need to complete self-assessments or undergo independent certification.

Organisations within scope should review their cloud environments, identify gaps in existing security measures, and document their remediation activities.

**Explore the NCSA's guidance and assessment pathways**




# 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, and the opportunity to work for a **Great Place to Work-Certified™** company, **recognised as one of the UK's Best Workplaces™ for medium-sized businesses**, **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