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 in post-16 education: Data protection guide for providers

Artificial intelligence is becoming an increasingly common part of post-16 education, supporting everything from lesson planning and learner support to administrative tasks and workforce management. As adoption grows, education providers must ensure AI is used responsibly and in line with UK data protection law.

In our latest guide, we explore five practical steps to help further and higher education providers strengthen AI governance, protect personal data, improve transparency, and equip staff to use AI responsibly.

Read our blog

UNITED STATES & CANADA

US Senators propose AI transparency protections for older adults

On 23 July 2026, US senators introduced the Senior Chatbot Protection Act. The Bill aims to protect older adults from deceptive AI interactions by requiring chatbot providers to:

- Clearly disclose when users are communicating with artificial intelligence
- Implement additional warnings for conversations involving health care and estate planning

- Obtain express consent before collecting or sharing personal information during chatbot interactions

Organisations developing or deploying AI chatbots should continue monitoring legislative developments and consider whether existing transparency and Privacy Notices remain fit for purpose as AI-specific regulation evolves.

Read our practical guide to updating Privacy Notices for AI

WestJet cyberattack highlights social engineering risks

The Office of the Privacy Commissioner of Canada (OPC) has published a compliance letter following its investigation into the 2025 cyberattack on WestJet, confirming the airline has committed to strengthening its cybersecurity measures. The breach affected the personal information of approximately 5.2 million customers and employees after a threat actor gained unauthorised access to WestJet's systems using social engineering techniques to bypass security controls.

Cyberattacks increasingly rely on social engineering rather than technical vulnerabilities alone, with AI enabling criminals to create more convincing phishing emails, impersonate trusted colleagues through voice cloning, and automate highly targeted attacks at scale. As these techniques become more sophisticated, organisations should ensure employees are equipped to recognise emerging threats alongside maintaining robust technical controls and incident response procedures.

Learn how to protect your organisation

California launches first sector-wide privacy audit

On 21 July 2026, the California Privacy Protection Agency (CPPA) launched its first sector-wide privacy audit, focusing on platforms that connect customers with independent workers, such as ride-hailing and food delivery services. It marks a new phase of proactive oversight under the California Consumer Privacy Act (CCPA) and will examine whether gig economy platforms are complying with individuals' rights to access and control their personal information, including how they handle requests from both consumers and workers.

The audit reflects CPPA's intention to use its new Audits Division to identify compliance issues across entire sectors rather than relying solely on complaints and enforcement investigations. The agency has confirmed this is the first of a series of sectoral audits, signalling that organisations across all industries should ensure their privacy programmes, data subject rights processes, and governance arrangements are ready to withstand regulatory scrutiny.

Read more about the audit

UNITED KINGDOM

UK Government launches Call for Evidence on international data transfers

The consultation seeks practical insights into whether the UK's current framework enables trusted cross-border data flows, with responses informing future policy developments. It focuses on four key themes:

- Awareness and behaviours around international transfers
- The understanding and use of transfer mechanisms
- Balancing compliance with accountability
- Ensuring trust in the face of a changing world

The Government is particularly keen to hear from those directly involved in international data transfers, including Data Protection Officers (DPOs) and senior decision-makers responsible for organisational strategy, although the Call for Evidence is open to all interested parties.

Respond to the consultation, which closes on 9 September 2026.

EUROPEAN UNION

EU AI Act transparency rules take effect on 2 August 2026

The EU's Digital Omnibus on AI entered into force on 27 July 2026, confirming revised compliance deadlines for high-risk AI systems and introducing measures to simplify certain administrative requirements. However, organisations should not assume the changes delay all obligations under the EU AI Act.

From 2 August 2026, the AI Act's transparency requirements apply, requiring organisations to clearly identify when people are interacting with AI or encountering certain AI-generated or manipulated content. Whilst some machine-readable marking requirements have been deferred for existing generative AI systems, most Article 50 obligations remain unchanged. Organisations providing or using AI in the EU should review their existing deployments now to ensure appropriate transparency measures are in place.

Read our summary of the latest AI Act updates

Italian DPA fines data broker €2M for GDPR violations

The Italian Data Protection Authority (Garante) has fined US-based data broker Lusha €2 million for unlawfully processing the personal data of individuals in Italy. The regulator found that Lusha:

- Collected, monitored, and sold personal data without a valid legal basis
- Breached the GDPR's principles of lawfulness, fairness, transparency, and data minimisation

Alongside the fine, the Garante ordered the company to stop processing the data and delete the personal data it holds relating to individuals in Italy.

The decision serves as a reminder that publicly available information is not automatically free to collect, enrich, and commercialise. Organisations using third-party contact databases should ensure providers can demonstrate how personal data has been obtained and processed lawfully, particularly where it has been sourced through web scraping or other large-scale data collection methods.

Read more about the Garante's decision

INTERNATIONAL

OAIC updates facial recognition guidance

The Office of the Australian Information Commissioner (OAIC) has updated its **guidance** on the use of facial recognition technology (FRT), providing organisations with clearer expectations for assessing privacy risks. The guidance reinforces that FRT is highly

privacy-invasive and should only be used where organisations can demonstrate that its use is necessary, proportionate, and compliant with the Australian Privacy Principles.

The updated guidance encourages organisations to undertake formal privacy risk assessments before deploying FRT, consider whether less intrusive alternatives are available, and ensure appropriate transparency measures are in place. Organisations using, or considering using, FRT should review the revised guidance to ensure their governance, documentation and privacy controls remain fit for purpose.

Explore our guide to facial recognition and data protection compliance.

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 (United Kingdom)**
- **Data Protection Officer - Life Sciences (United Kingdom)**
- **Data Protection Support Officer (United Kingdom)**
- **Data Protection Officer (The Netherlands)**
- **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