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.

A practical guide to updating Privacy Notices for AI

For organisations deploying AI systems that process personal data, transparency is becoming one of the most challenging areas of compliance. As AI moves into recruitment, customer support, risk assessment, and other core business functions, Privacy Notices are now expected to explain not just what data is used, but how AI influences decisions and outcomes for individuals.

In this blog, we break down what meaningful transparency looks like in practice under both the GDPR and the EU AI Act. We highlight the areas Privacy Notices most often fall short and set out a practical framework to help organisations keep their disclosures clear, accurate, and aligned with evolving regulatory expectations.

Read our blog

UNITED KINGDOM

Government to upskill 10M workers through AI training

On 28 January 2026, the UK government announced the expansion of its AI Skills Boost programme. The fourteen free online courses are designed to give adults the practical skills needed to use AI tools effectively in the workplace. Available to anyone in the UK via the AI Skills Hub, the initiative aims to upskill 10 million workers by 2030 and position Britain as the fastest-adopting AI country in the G7.

As AI skills move from a specialist capability to a baseline workplace competency, organisations are likely to see AI use extend into routine workflows, from drafting content and analysing data to summarising meetings and supporting decision-making. This shift increases the need to move beyond high-level AI policies and towards practical, role-based controls that maintain visibility over data use, third-party tools, and how AI outputs influence business decisions.

Read our blog for more on building AI governance at scale.

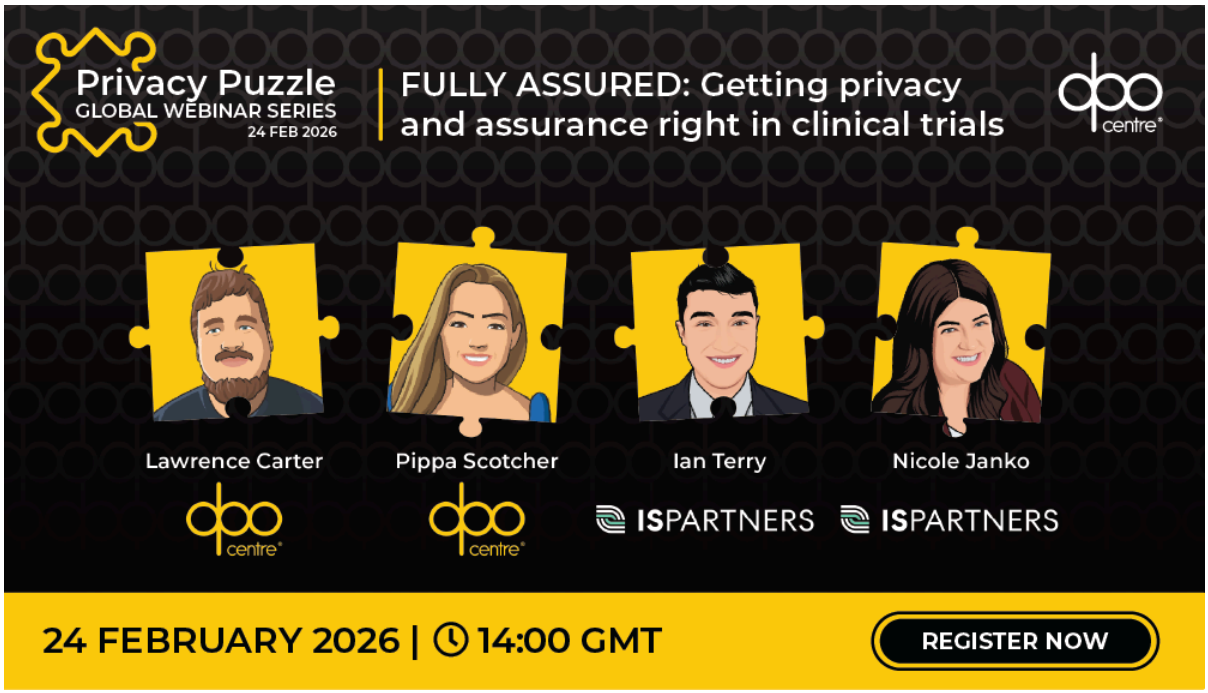
ICO updates guidance on international transfers under UK GDPR

Aimed at making the rules easier for organisations to apply in practice, the updated guidance includes:

- A 3-step test to help identify whether organisations are making restricted transfers, supported by FAQs
- Clarified roles and responsibilities for complex controller-processor chains
- A glossary to support organisations with limited knowledge of international transfers

For compliance teams, the update places greater emphasis on documenting transfer decisions, safeguards, and risk assessments. As international data use becomes more embedded in routine operations, organisations should expect regulators such as the Information Commissioner's Office (ICO) to look for clear, auditable evidence that restricted transfers have been identified and governed consistently.

Read the ICO guidance



EUROPEAN UNION

CNIL publishes final recommendations on multi-device consent

On 16 January 2026, France's data protection authority (CNIL) published guidance on how organisations can manage cookie and tracker consent across multiple devices when users are logged into a single account. The recommendations explain how a choice made on one device can apply to others (such as phones, tablets, computers, and connected TVs), provided users are clearly informed and remain in control of their preferences.

For organisations, this means ensuring that:

- Consent choices work consistently across all devices (accept, refuse, and withdraw apply everywhere)
- Users are clearly told up front that their choice will apply across their logged-in devices
- Banners and preference settings reflect this wider scope

Where a user signs in on a new device, the CNIL also expects organisations to remind them of their existing choices and offer a way to resolve any differences between pre-login and account-level preferences. Whilst multi-device consent remains optional, where it is used, it should be documented and easy for users to review and change across every logged-in environment.

Read the CNIL's recommendation

EDPB updates FAQs on EU-US Data Privacy Framework for European businesses

Published on 23 January 2026, version 2 expands the practical guidance available to European organisations that rely on the framework to transfer personal data to the United States. The update shifts the focus from high-level eligibility to operational accountability, clarifying how organisations should assess certification, manage vendor relationships, and document compliance across their transfer arrangements.

For in-scope organisations, the FAQs set out clearer expectations around what must be done in practice, including:

- Verifying active self-certification of US recipients and its scope, particularly where HR data is involved
- Ensuring onwards transfer safeguards flow down through the vendor and sub-processor chain
- Aligning internal policies, contracts, and governance with the DPF principles
- Using alternative transfer tools, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), where certification does not apply or lapses

Regulators will look for clear, auditable evidence that certification checks and vendor oversight are embedded into routine transfer governance rather than treated as a one-off compliance step.

Read the FAQs

Dutch DPA warns against permanent camera monitoring of transport employees

On 28 January 2026, the Dutch data protection authority (AP) published guidance on the use of cameras at employees' fixed workstations in public transport, following a complaint involving bus operator Arriva. The AP confirmed that permanent or structural camera surveillance of employees is not permitted, and that cameras cannot be used for the systematic monitoring, assessment, or evaluation of staff.

The AP set out clear expectations for employers, particularly in public and freight transport:

- Only use cameras where strictly necessary, such as during safety-related incidents
- Establish technical measures to prevent employees from being continuously in view
- Clearly define and communicate the purpose, retention periods, and access rights for camera footage
- Be transparent with staff about how and when monitoring may occur

The guidance reinforces the need to balance operational security with employee privacy. Learn more about the boundaries of employee monitoring in our latest webinar.

Watch on demand

CANADA & UNITED STATES

New York Senate passes Bill to strengthen health information privacy

On 27 January 2026, the New York State Senate passed Senate Bill S1633A — legislation to amend the state's Public Health Law and strengthen privacy protections for sensitive health information. The Bill would give patients control over how their health data is shared, establishing a right for patients to request restrictions on the disclosure of their health information.

Health Information Networks (HINs), electronic health record (EHR) systems, and healthcare providers will be required to develop the capability to limit the sharing of sensitive, codified information, whilst allowing other data to continue to support treatment, payment, and healthcare operations. Healthcare providers are expected to support these rights by informing patients of their options and complying with any restrictions they request.

Read the Bill

Ontario IPC publishes guidance on AI scribes in Healthcare

On 28 January 2026, the Information and Privacy Commissioner of Ontario (IPC) released new guidance and a practical checklist for health organisations using AI scribes — tools that record, transcribe, and summarise patient consultations. The guidance highlights that whilst these systems can reduce administrative burden, they also introduce heightened privacy, security, and human rights risks.

For in-scope organisations, the IPC sets clear expectations around governance and accountability, including:

- Establishing an AI governance framework before deployment, covering risk, policies, and human oversight
- Maintaining Privacy Impact Assessments (PIAs) and updating them when systems or purposes change
- Strengthening vendor due diligence and contracts, including controls on data use and training
- Applying data minimisation and retention limits
- Training staff and managing ‘shadow AI’ risks, with clear breach reporting routes

Compliance teams should not treat AI scribes as simple productivity tools. Regulators are likely to expect documented, ongoing oversight across the full AI lifecycle, from procurement and configuration to day-to-day use and decommissioning. Organisations should be able to evidence that patient privacy and accountability remain central to how these systems are governed.

Download the guidance and checklist

INTERNATIONAL

South Korea’s AI Basic Act and Enforcement Decree take effect

On 22 January 2026, South Korea’s AI Basic Act and its subordinate Enforcement Decree came into force, creating a comprehensive national AI framework. The law and accompanying decree set out high-level requirements for AI safety, transparency, and accountability, and establish the groundwork for further detailed rules to be issued by the Ministry of Science and ICT (MSIT).

Organisations involved in developing or providing AI systems must begin aligning with their obligations under the Act, including:

- Transparency and safety responsibilities for high-impact and generative AI

- Advance user notice and output labelling so AI-generated content can be clearly identified
- Risk management and internal measures to assess, document, and mitigate potential harms

Whilst the full set of technical requirements and implementation details are still being finalised by MSIT, organisations using AI in the South Korean market should be preparing compliance plans, reviewing governance frameworks, and assessing how their AI systems qualify under the law's definitions and risk categories.

[Learn more about the AI Basic Act]

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 Coordinator - Life Sciences (Poland)**
- **Data Protection Support Officers (United Kingdom)**
- **Senior Commercial Executive (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