the dpia

GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE

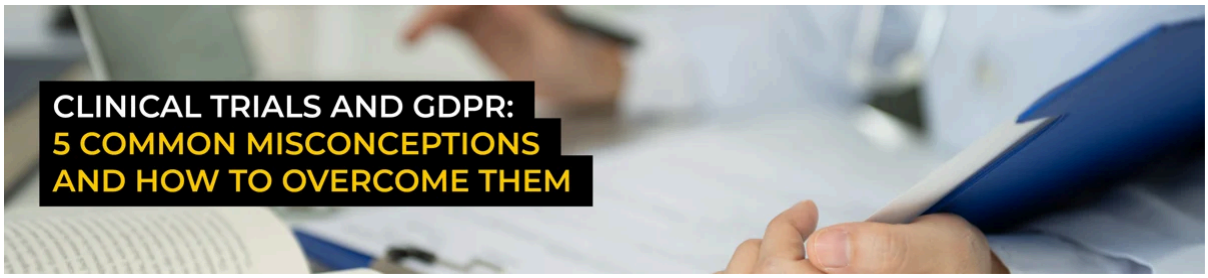
The DPIA is an assessment of the impact of the most significant and important-to-know data protection issues from around the globe. It's not the full story, just a quick 3-minute read, collated and condensed to keep you updated with the latest news in our ever-evolving industry.

Clinical trials and GDPR: 5 common misconceptions and how to overcome them

In clinical trials, GDPR compliance is often seen as a late-stage hurdle rather than a core design consideration. In reality, many trial delays don't stem from the regulation itself but from misunderstandings about responsibility, scope, and timing.

Our latest blog explores five common GDPR misconceptions in clinical trials and outlines practical steps to overcome them. We explain how to clarify responsibilities, assess scope, manage pseudonymisation risks, ensure DPO independence, and embed GDPR governance early to avoid delays.

Read our blog



UNITED KINGDOM

ICO joins global statement on privacy risks of AI-generated imagery

Signed by 61 data protection authorities, the statement addresses the privacy risks of AI-generated images and videos depicting identifiable individuals without their knowledge or consent. It reminds organisations that AI content generation systems must comply with applicable data protection laws and outlines four guiding principles:

- Implement safeguards to prevent misuse of personal data
- Ensure meaningful transparency about system capabilities and risks

- Provide accessible mechanisms for individuals to request removal of harmful content
- Introduce enhanced protections for children

The initiative reflects growing global concern about the misuse of generative AI and reinforces expectations that developers and deployers act responsibly.

Read the statement

Court of Appeal rules on DSG Retail data breach case

On 19 February 2026, the UK Court of Appeal upheld the Information Commissioner's appeal in the DSG Retail case. The ruling confirms that organisations must implement appropriate security measures to protect personal data from unauthorised access, even where the data may not be directly identifiable to attackers.

The judgement reinforces that security obligations focus on the controller's responsibility to safeguard data, not solely on whether an attacker can immediately identify individuals. For organisations, it clarifies that compromised data may still qualify as personal data in a breach context, particularly where re-identification is possible through combination with other information.

Read the decision

EUROPEAN UNION

EDPB launches coordinated enforcement action on the right to erasure

The European Data Protection Board (EDPB) has published the outcome of its 2025 Coordinated Enforcement Action examining how organisations implement the right to

erasure under the General Data Protection Regulation (GDPR). The exercise involved 32 supervisory authorities and 764 controllers across the European Economic Area.

Overall compliance was assessed as ‘average’ with seven recurring weaknesses identified, including gaps in internal procedures, inconsistent retention practices, and difficulties deleting data in backups.

The findings signal that regulators continue to prioritise **Article 17** compliance. For organisations, it is a reminder that erasure processes must be clear, documented, and consistently applied in practice.

Read the 2025 Coordinated Enforcement Action

Italian DPA fines eCampus for facial recognition failures

Italy’s Data Protection Authority (Garante) has fined eCampus €50,000 for unlawfully using facial recognition to verify student attendance. The university processed the biometric data of more than 450 trainees per lecture, making course participation conditional on consent.

The Garante found that consent was not a valid legal basis in this context, as students could not freely refuse processing, and no specific law authorised the use of biometric data for attendance monitoring. It also identified disproportionate retention periods and the absence of a Data Protection Impact Assessment (DPIA) prior to deploying the system.

For organisations, the decision reinforces that biometric systems require a clear legal basis and a DPIA before deployment, particularly where participation or access depends on the processing.

What is a DPIA?

Dutch DPA warns against using autonomous AI agents

On 12 February 2026, the Dutch Data Protection Authority (AP) warned organisations against using AI agents containing privacy-sensitive or confidential data, such as OpenClaw. The AP cautioned that such systems have full access to users’ computers, can act independently without prior human approval, and may fail to meet basic security requirements, creating significant risks of data breaches and account takeovers.

The warning underscores growing regulatory concern around AI agents with broad system access and limited oversight. Organisations deploying such tools must carefully assess security, access controls, and accountability before implementation.

Read our blog for practical guidance on governing AI agents.

CANADA & UNITED STATES

US Department of Labor releases AI Literacy Framework

The framework is intended to guide nationwide AI literacy efforts across workforce and education systems, providing a structured foundation for developing AI skills while allowing flexibility across industries, roles, and educational contexts. It sets out five core content areas — understanding AI principles, exploring AI use cases, directing AI effectively, evaluating AI outputs, and using AI responsibly — alongside seven delivery principles to support programme design and implementation.

For organisations, the framework reflects growing expectations that AI adoption is supported by workforce education, structured governance, and responsible use practices rather than ad hoc deployment.

Download the AI Literacy Framework

OPC issues statement on AI-related privacy risks

The Office of the Privacy Commissioner of Canada (OPC) has told the Standing Committee on Access to Information, Privacy and Ethics that managing AI-related privacy risks is now a strategic priority. It warned that the rapid expansion of artificial intelligence and its reliance on personal data raises significant privacy challenges and that public trust will be critical to AI's long-term success.

The OPC urged organisations to embed Privacy by Design, ensure transparency about how AI is used, and remain accountable for AI-driven decisions affecting individuals.

AI Impact Assessments (AIIAs) can help organisations identify and mitigate AI-related privacy risks at an early stage. **Read our blog** to learn more.

INTERNATIONAL

South Korea launches AI Privacy Public-Private Policy Council

The 37-member council will address emerging privacy risks linked to agent-based and physical AI technologies, focusing on data processing standards, risk management, and the protection of data subject rights. It will analyse AI service flows, identify risks, and propose safeguards to support the effective exercise of rights in autonomous environments.

The outcomes will be shared with national AI policy bodies and research institutes to strengthen implementation of South Korea's broader AI strategy.

For organisations, the initiative signals increasing regulatory scrutiny of governance frameworks for advanced AI systems.

Learn more

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)**

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