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.

Privacy compliance vs assurance in clinical trials: Why you need both

For organisations running clinical trials, meeting regulatory requirements is only part of the challenge. Sponsors, partners, and regulators increasingly expect evidence that privacy and security controls are not only in place but operating effectively in practice.

Our latest blog explains the distinction between privacy compliance and assurance, why it causes delays in clinical trials, and how organisations can strengthen their approach to meet growing expectations.

Read our blog

UNITED KINGDOM

ICO publishes guidance on 'recognised legitimate interests'

On 23 March 2026, the Information Commissioner's Office (ICO) published **new guidance** on 'recognised legitimate interests' (RLI) as a lawful basis for processing personal data.

The guidance explains how RLI differs from the standard Legitimate Interests basis, setting out a list of pre-approved public interest purposes that organisations can rely on without carrying out a balancing test. It also outlines the five RLI conditions, when they apply, and how organisations may share personal data under this framework.

Organisations should assess whether their processing activities genuinely fall within the defined RLI conditions and ensure they can clearly justify its use.

Learn more about the ICO's guidance and what it means in practice.

Guardian investigation finds UK Biobank health data exposed online

The investigation found that researchers inadvertently published datasets whilst sharing their work. The data did not include names or addresses, but one dataset contained detailed hospital diagnoses and dates for more than 400,000 participants, along with their sex, month, and year of birth.

Privacy experts have raised concerns about the risk of re-identification, noting that seemingly limited data points can be cross-referenced with other publicly available information. However, UK Biobank rejected this, stating that no identifying data was provided to researchers and that no individuals have been identified.

The incident highlights the challenges of maintaining control over data once access is granted to third-party researchers, particularly where datasets contain confidential health information.

Read our blog on pseudonymisation and risk reduction.

EUROPEAN UNION

CJEU clarifies when DSARs may be considered 'abusive' under GDPR

The Court of Justice of the European Union (CJEU) has ruled that a Data Subject Access Request (DSAR) may be considered 'excessive' — and therefore refused — where it is made solely to secure compensation, rather than to exercise data protection rights.

The case involved an Austrian individual who submitted a DSAR to an optician after subscribing to its newsletter. The request was refused, with evidence suggesting a pattern of similar requests followed by compensation claims. The individual subsequently sought €1,000 in damages, alleging harm from the refusal.

The CJEU confirmed that even a first access request may be deemed excessive in certain circumstances, provided the controller can demonstrate the abusive intent.

This ruling provides organisations with a clearer basis for challenging requests that are manifestly abusive. However, controllers must be able to evidence their reasoning and should proceed with caution before refusing to respond.

Download our white paper for advice on handling DSARs.

EDPB launches 2026 Coordinated Enforcement Framework

Announced by the European Data Protection Board (EDPB) on 19 March 2026, the CEF will focus on how organisations meet their transparency and information obligations under the General Data Protection Regulation (GDPR). The initiative will assess compliance with Articles 12-14, which require organisations to provide clear, accessible information about how personal data is collected and used.

A total of 25 Data Protection Authorities across Europe will take part, contacting organisations through enforcement actions or fact-finding exercises to evaluate how these requirements are implemented in practice.

Organisations should review their Privacy Notices to ensure they are clear, concise and accurately reflect current processing activities, particularly where data is collected indirectly or used for new purposes.

Read our blog on drafting GDPR-compliant Privacy Notices.

Dutch DPA publishes guidance on health data in the cloud

On 23 March 2026, the Dutch Data Protection Authority (AP) published a **practical guide** on the use of cloud services for processing health data, highlighting key risks and compliance expectations for healthcare providers.

The guidance emphasises the need for robust risk assessments, strong oversight of cloud providers, and clear contractual arrangements. It also reinforces the importance of maintaining control over data, including ensuring secure exit strategies and compliance with international transfer rules.

The AP's guidance reflects increasing regulatory focus on how organisations manage third-party risk in cloud environments, particularly for high-risk processing. Organisations should have well-defined Data Processing Agreements (DPAs) that clearly set out roles, responsibilities, and safeguards.

Read our guide to DPAs

CANADA & UNITED STATES

White House unveils National Policy Framework for Artificial Intelligence

The framework outlines proposals for a coordinated approach to AI regulation across the US.

It sets out six key objectives and includes a series of recommendations to Congress, focusing on areas such as:

- Age assurance requirements for AI services likely to be accessed by minors
- Safeguards to reduce risks of exploitation and harm
- Strengthened enforcement against AI-enabled fraud and impersonation

It also proposes the introduction of federal protections against the unauthorised use of AI-generated digital replicas, as well as measures to make government datasets more accessible for training AI systems.

The framework signals a shift toward more structured federal oversight of AI, with potential implications for organisations developing or deploying AI systems in the US.

Read the framework

Canada introduces lawful access bill for service providers

On 12 March 2026, Canada introduced Bill C-22 to the House of Commons. Known as *an Act respecting lawful access*, the Bill applies to telecommunications and electronic service providers and sets out a framework for law enforcement to obtain access to subscriber

information and computer data through service demands, production orders, and warrants.

The Bill defines key terms, such as *subscriber information* and *public officer*, and introduces the Supporting Authorized Access to Information Act (SAAIA), establishing compliance requirements and penalties for non-compliance.

Organisations in scope should ensure they have the technical capability to respond to lawful access requests in line with the proposed framework.

Read the Bill

INTERNATIONAL

South Korea strengthens PIPA

South Korea has approved amendments to its Personal Information Protection Act (PIPA), aimed at strengthening deterrence against poor data handling and driving greater investment in governance.

Key changes include:

- Increased penalties for repeat or serious breaches, rising to up to 10% of annual turnover
- Broader incident reporting requirements, including forgery and personal data damage, alongside prompt notification obligations to affected individuals
- Expanded accountability for senior leadership
- Mandatory security and privacy certification (ISMS-P) for organisations with significant data protection impact

Most provisions will take effect on 11 September 2026, with certification requirements applying from 1 July 2027.

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 - Life Sciences (United Kingdom)**
- **Data Protection Coordinator - Life Sciences (Poland)**
- **Financial Controller (United Kingdom)**
- **Senior Commercial Executive (United Kingdom)**
- **Senior HR Advisor - maternity cover (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, **recognised as one of the UK's Best Workplaces™ for medium-sized businesses**, **apply today!**

FOLLOW US ON LinkedIn