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.

Marketing compliance under DUAA and PECR

The Data Use and Access Act 2025 (DUAA) has significantly increased the financial consequences of non-compliance with the Privacy and Electronic Communications Regulations (PECR). With maximum fines now aligned to UK GDPR, organisations should no longer treat email marketing, cookies, and online tracking as lower-risk compliance issues.

In our latest blog, we explore the changes introduced by the DUAA and outline the practical steps marketing teams should take to reduce compliance risk.

Read our blog

UNITED KINGDOM

NHS England issues guidance on unlawful access to patient records

NHS England has launched a campaign warning health and care staff that accessing patient records without a legitimate work-related reason can lead to dismissal, professional sanctions, or criminal prosecution. The campaign follows several incidents involving unauthorised access to the records of individuals connected to high-profile events.

The guidance explains the different forms of unlawful access and sets out how organisations can prevent, identify, and investigate inappropriate activity. It highlights that protecting sensitive records requires more than restricting access. Organisations must

also monitor how permissions are used, educate staff about acceptable access, and act consistently when concerns arise.

Read the NHS guidance

UK plans new safeguards for young social media users

On 15 July 2026, the UK Government announced plans to introduce default overnight social media curfews and switch off certain addictive platform features for 16- and 17-year-olds. The measures form part of wider proposals to strengthen online protections for young people, including reducing exposure to features such as infinite scrolling and autoplay.

Organisations should consider how digital services are designed, particularly where children and young people are affected. Privacy, transparency, and user wellbeing are integral to responsible platform design, alongside traditional data protection requirements.

Learn more about the Government's proposals

EUROPEAN UNION

EDPS publishes checklist for human oversight of AI

The European Data Protection Supervisor (EDPS) has published a practical checklist to help organisations assess the effectiveness of human intervention in automated decision-making. Whilst the checklist is not a formal compliance tool, it highlights the operational measures that can strengthen meaningful human oversight.

With human oversight a core requirement under both the GDPR and the EU AI Act, organisations that treat it as an operational discipline rather than a governance formality

will be better placed to demonstrate that automated decisions remain fair, transparent, and accountable.

[View the checklist]

EDPB published draft guidelines on anonymisation

Open for consultation until 20 October 2026, the guidelines provide further clarity on when personal data can be considered anonymous. Building on recent case law, they explain that identifiability should be assessed from the perspective of the recipient, considering whether they have any reasonable means of re-identifying individuals.

The long-awaited guidance provides a practical framework for assessing anonymisation and is particularly relevant for organisations that share, disclose, or reuse datasets. Understanding when data is genuinely anonymous can help organisations make more informed decisions about data sharing and their ongoing data protection obligations.

[Read the guidelines]

Dutch DPA publishes resources for compliant generative AI

The Dutch data protection authority, Autoriteit Persoonsgegevens (AP), has published two practical resources to help organisations develop and deploy generative AI in line with the GDPR. The guidance is aimed at both developers and organisations using AI systems, covering key privacy considerations throughout the AI lifecycle.

The resources are designed to help organisations identify privacy risks early, implement appropriate safeguards, and embed data protection into AI projects from the outset. As generative AI adoption continues to grow, guidance such as this can help organisations demonstrate accountability and support responsible AI governance.

[Download the resources]

Connecticut's new law regulates facial recognition technology

From 1 October 2026, organisations using facial recognition technology for security purposes in Connecticut will be subject to new transparency requirements. Public Act No. 26-64 requires businesses to clearly inform individuals when facial recognition is in use and provide access to a facial recognition policy explaining how the technology is used.

The new requirements reflect growing regulatory expectations around the use of biometric technologies. Organisations deploying facial recognition should ensure individuals are informed about its use, understand when consent may be required, and implement appropriate governance to support lawful and transparent processing.

Watch our webinar on the privacy risks of FRT

Canada publishes guidance on information sharing codes of practice

The Privacy Commissioner of Canada has published guidance to help organisations develop codes of practice for sharing personal information under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). Following legislative changes in March 2025, financial reporting entities that wish to share personal information without an individual's knowledge or consent in the limited circumstances permitted by the Act must:

- Establish a code of practice governing that information sharing
- Obtain approval from the Privacy Commissioner before relying on the new provisions

Organisations should ensure personal data is only shared where there is a clear legal basis, appropriate safeguards are in place, and the purposes and responsibilities for sharing are clearly documented.

Read the guidance

INTERNATIONAL

Mauritius requires in-house DPOs from 2027

Mauritius has introduced new regulations that strengthen the role of the Data Protection Officer (DPO), with the changes taking effect on 1 January 2027. Organisations that are required to appoint a DPO will no longer be able to rely on an outsourced provider and must instead designate a suitably qualified employee to fulfil the role.

The regulations also introduce new requirements around DPO qualifications, notification to the Data Protection Office, and publication of the DPO's contact details. Organisations operating in Mauritius should review their current arrangements well ahead of the implementation date to ensure they can meet the new requirements.

Learn more about the new DPO requirements

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 Coordinator - Life Sciences (Poland)**
- **Data Protection Officer - 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