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.

UK charity soft opt-in: What charities need to know

The introduction of the charity soft opt-in has given charities greater flexibility to engage with supporters through electronic marketing. However, many organisations remain cautious about adopting the exemption due to practical challenges around implementation, governance, and supporter expectations.

In our latest blog, we explore why some charities have delayed introducing the charity soft opt-in, explain the ICO's latest guidance, and outline the practical steps charities should take before relying on the exemption.

Read our blog

UNITED KINGDOM

High Court rules work messages on personal devices can be disclosable

A recent High Court decision has confirmed that business communications held on personal devices, including messaging apps such as WhatsApp and iMessage, may still be subject to disclosure in litigation. The ruling found that mixing personal and business messages on the same device does not, by itself, put company-related communications beyond reach.

The decision is a timely reminder for organisations to understand where business communications take place and ensure they can identify, preserve, and retrieve relevant data when needed, particularly where personal devices are used for work purposes.

[Read our blog to understand how to manage the risks of BYOD]

Guernsey's DPA issues sanction for DSAR failings

The regulator sanctioned the Committee for Health & Social Care after finding 'systematic issues' in its handling of Data Subject Access Requests (DSARs). An inquiry found the organisation repeatedly failed to respond to DSARs or communicate extensions within the required statutory timeframes.

The case highlights the importance of having clear procedures in place to identify, track, and respond to requests on time. Clear ownership, documented workflows, and regular training can help prevent individual requests from becoming wider compliance issues.

[Download our DSAR guide]

EUROPEAN UNION

Spain’s DPA issues record fine of €18M for GDPR breaches

Spain's data protection authority (AEPD) has fined travel technology provider Amadeus €18 million for breaching Articles 6 and 14 of the General Data Protection Regulation (GDPR). The company reused customer data to develop a new traveller profiling platform but failed to identify a valid lawful basis and provide individuals with sufficient information about the new processing activities.

The decision serves as a reminder that personal data collected for one purpose cannot automatically be reused for another. Organisations looking to develop new products, services, or insights using existing customer data should assess whether the new processing is compatible with the original purpose, identify an appropriate lawful basis, and ensure individuals receive clear and transparent privacy information.

Read our blog on writing clear and compliant Privacy Notices

Court rules businesses are responsible for chatbot responses

A German court has ruled that organisations can be held responsible for misleading statements made by AI chatbots on their websites. The case involved a medical practice whose chatbot incorrectly described the qualifications of two doctors, with the court finding that the chatbot's responses formed part of the organisation's own communications.

The decision reinforces the importance of testing, monitoring, and governing customer-facing AI systems. Organisations deploying AI chatbots should ensure appropriate safeguards, oversight, and review processes are in place to reduce the risk of inaccurate or misleading responses.

Download our guide to deploying LLMs with confidence

Dutch DPA consults on DPIA exception list

Autoriteit Persoonsgegevens (AP) is consulting on a proposed list of processing activities that would not require a Data Protection Impact Assessment (DPIA).

The AP is seeking input from SMEs, independent entrepreneurs, and experts before the list is finalised and submitted to the European Data Protection Board (EDPB) for review. The aim is to reduce regulatory burden for smaller organisations and self-employed individuals by providing greater clarity on when a DPIA is not required.

The consultation highlights the importance of proportionate, risk-based compliance and ensuring DPIA requirements remain focused on processing activities likely to result in high risk.

Respond to the consultation

UNITED STATES & CANADA

EU-US Data Privacy Framework faces renewed scrutiny

The European Commission is assessing the implications of the recent US Supreme Court ruling in *Trump v. Slaughter* following concerns raised by privacy campaign group noyb. The organisation argues that the judgement may weaken one of the key legal foundations of the EU-US Data Privacy Framework (DPF), which relies on the US Federal Trade Commission (FTC) acting as an independent enforcement authority.

The current EU-US adequacy decision remains in force, and organisations can continue relying on the DPF for transatlantic data transfers. However, the development highlights the importance of monitoring international data transfer mechanisms as legal and regulatory frameworks continue to evolve.

Read noyb's letter to the European Commission

OIPC sets privacy priorities for next three years

The Office of the Information and Privacy Commissioner for British Columbia (OIPC) has published its Strategic Plan 2025–2028, *Trust in the Age of Information*. The plan identifies three strategic priorities:

1. Promoting trust and transparency in public institutions
2. Supporting trusted innovation in technologies, such as artificial intelligence and surveillance
3. Improving rights and equity for vulnerable groups

Whilst the plan does not introduce new legal obligations, it provides a clear indication of the areas likely to receive increased regulatory attention over the coming years. Organisations should continue to strengthen transparency, embed responsible AI governance, and ensure privacy programmes reflect the needs of vulnerable individuals.

[Read the Strategic Plan]

INTERNATIONAL

Five Eyes agencies warn AI is accelerating cyber risk

Five Eyes cyber security agencies have issued a joint statement warning that artificial intelligence is increasing the speed, scale, and sophistication of cyber threats. The agencies – representing Australia, Canada, New Zealand, the UK and US - urge leaders to treat cyber resilience as a core business risk, rather than a purely technical issue.

The statement recommends that organisations prioritise foundational cyber security controls, reduce unnecessary system access, accelerate patching, strengthen identity and access controls, and test incident response plans before breaches occur.

[Read the statement]

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)**
- **Content Marketing Specialist (United Kingdom)**
- **Senior HR Advisor - maternity cover (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

The DPO Centre Group
London | Amsterdam | Toronto | Dublin