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.

EU AI Act compliance part 3: Roles and requirements for North American organizations

In the third instalment of our blog series, we address the key question: Who is affected by the EU AI Act and what are the specific obligations? We break down the six distinct roles of the AI supply chain, including Providers and Deployers.

Given the EU AI Act's extra-territorial reach, any North American organization marketing, deploying, or using an AI system in the EU must adhere to this new legislation. Understanding these requirements is vital to ensure your organization meets compliance standards. Read on to find out what the obligations are and if you are affected.

Read the blog

CANADA & UNITED STATES

OPC launches Privacy Breach Tool

The Office of the Privacy Commissioner of Canada (OPC) has introduced a Privacy Breach Risk Self-Assessment Tool to help businesses and federal institutions evaluate whether a breach creates a real risk of significant harm to individuals. If so, the breach must be reported to the OPC and to the Treasury Board Secretariat (TBS) for federal bodies, and affected individuals must also be notified. The tool guides users through dynamic questions to assess breach severity based on factors like data type, number of individuals affected, and likelihood of misuse. While the tool does not provide an official or legally binding decision from the OPC, it offers valuable guidance to support breach response and compliance.

Unredacted JFK files cause significant data breach

A major data protection breach has occurred in the US following the release of largely unredacted JFK assassination files by the Trump administration. According to the Washington Post, the documents exposed the social security numbers, names, and addresses of over 400 individuals, including former congressional staffers, diplomats,

military personnel, and investigators from the 1970s Church and House Select Committees.

The breach highlights the ongoing risks around handling historic records and the need for rigorous redaction practices to protect personal data, even decades later.

Read our blog on applying GDPR to historic records

New US rule tightens restrictions on cross-border transfers

On 8 April 2025, the US Department of Justice's (DOJ) new rule on cross-border transfers came into effect. The rule restricts the transfer of US sensitive personal and government-related data to countries of concern, including China, Russia, Iran, Cuba, and North Korea. It applies to data brokerage, vendor, employment, and investment agreements, and introduces new privacy, cybersecurity, and governance obligations.

US companies must now assess whether their data qualifies as 'sensitive' or 'government-related' and ensure compliance. The reporting requirements include an annual report for certain restricted transactions involving cloud-computing services. With civil and criminal penalties for violation, including fines and imprisonment, the rule marks a major shift in cross-border data compliance and enforcement.

Read the DOJ statement

UNITED KINGDOM

Charities set to gain new direct marketing exemption

In an approved amendment to the proposed UK Data (Use and Access) Bill, charities will be allowed to send direct electronic marketing to new supporters without obtaining explicit consent, provided the messages align with the charity's mission and include clear opt-out options. This is similar to the current 'soft opt-in' rule that applies to commercial organisations under the Privacy and Electronic Communications Regulations (PECR).

With the bill looking set to pass as early as May 2025, charities should begin preparing by reviewing privacy notices and data systems, and crucially, conducting a Legitimate Interest Assessment (LIA). This is essential because the exemption could shift the lawful basis for processing data from Consent to Legitimate Interests. The Information Commissioner's Office has endorsed the change but urges careful and responsible implementation of the proposed changes.

View the progression of the DUA Bill

EUROPEAN UNION

DPC to fine TikTok over €500M for unlawful EU data transfers

TikTok's parent company, Bytedance, faces further penalties as Ireland's Data Protection Commission (DPC) prepares to issue a fine exceeding €500 million for violating GDPR. According to reporting by Bloomberg, TikTok allowed engineers in China to access personal data of European users without sufficient safeguards. The DPC is also likely to order TikTok to suspend the data processing within a defined period.

TikTok previously received fines totalling €345 million from the DPC for violating children's privacy and GDPR requirements, making this new fine the largest to date against the platform. It's a clear warning to other big tech firms handling EU personal data to ensure full compliance with cross-border data transfer rules.

Read our blog on EU and UK data transfer mechanisms

Germany opens door to GDPR claims under competition law

On 27 March 2025, Germany's Federal Court of Justice, Bundesgerichtshof (BGH) published three landmark rulings confirming that GDPR violations can also trigger legal claims under competition law. Following ECJ guidance, the BGH held that both competitors and consumer protection associations can bring actions for GDPR breaches under the Unfair Competition Act (UWG). This expands enforcement beyond regulators and data subjects.

While a surge in warning letters is unlikely due to restrictions on claims by smaller firms, businesses should review privacy notices and data practices to mitigate risks.

Read the rulings (in German)

INTERNATIONAL

Türkiye enacts new cybersecurity law

On 19 March 2025, Türkiye's new Cybersecurity Law (no. 32846) came into effect, marking a significant step in integrating cybersecurity into national security. The law introduces strict obligations for public and private entities handling personal data or critical infrastructure, including mandatory reporting of incidents, use of certified cybersecurity providers, and regulatory oversights by the newly established Cybersecurity Presidency and Cybersecurity Board.

The Law defines key cybersecurity terms and requires compliance across all stages of digital operations. Various administrative and criminal penalties apply for non-compliance, including failure to maintain confidentiality, potentially leading to between 4 and 8 years in prison.

For organisations engaging with Turkish partners or data flows, this law raises the bar for cybersecurity standards and data governance.

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 Privacy Officers (Canada)**
- **Data Protection Officers (United Kingdom/ The Netherlands)**
- **Data Protection Officers - Life Sciences (United Kingdom/Europe/Canada)**
- **Data Protection Support Officers (United Kingdom)**

If you are looking for a new and exciting challenge, **apply today!**

FOLLOW US ON LinkedIn