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.**

# Pseudonymisation under the GDPR: What the latest EU ruling means for organisations

A new ruling by the Court of Justice of the European Union could reshape how organisations classify and share pseudonymised data. The Court confirmed that if a recipient cannot reasonably re-identify individuals, the data may fall outside the GDPR's scope, potentially easing compliance in certain data-sharing scenarios.

For organisations that rely on coded datasets, particularly in research and clinical settings, this shift could mean greater flexibility but also greater responsibility to prove that re-identification isn't possible. Our latest blog explains what the judgment means for Life Sciences organisations and provides practical steps to maintain confidence in data-sharing processes.

**Read our blog**


## CANADA & UNITED STATES

# IPC releases revised De-Identification Guidelines for Structured Data

Published on 15 October 2025 by the Information and Privacy Commissioner of Ontario (IPC), the revised guidance updates the province's approach to de-identifying structured data. It aims to help organisations balance data utility with privacy protection amid new technologies, emerging risks, and evolving regulatory standards.

The updated guidelines complement international standards and provide practical tools to support responsible data sharing and reuse. They:

- Define key concepts such as pseudonymisation vs de-identification, direct and indirect identifiers, and the identifiability spectrum
- Address public and non-public data release models and explain how risk assessments vary by context and controls
- Recommend model-based risk assessments with defined thresholds for acceptable risk levels
- Include detailed checklists for mitigating controls, data sharing agreements, and documentation requirements

The IPC also outlines a 12-step process for de-identifying structured data, helping organisations ensure transparency, accountability, and Privacy by Design.

**Download the guidelines**

---

# Car insurers fined $14.2M in New York data breach case

An investigation by the Office of the New York State Attorney General (OAG) uncovered major security failures at eight auto insurers, exposing the personal information of more than 825,000 residents. The OAG found that the companies' online quoting tools allowed external agents to exploit a pre-fill function, exposing private data, including driver's licence numbers and dates of birth. Some of the stolen information was later used to file fraudulent unemployment claims during the COVID-19 pandemic.

As part of the settlement, the companies must adopt new measures to strengthen their information governance practices, including:

- Maintaining a comprehensive information security programme to protect private information
- Developing and maintaining an inventory of personal data and associated protections
- Enforcing strong authentication procedures and access controls
- Implementing monitoring and alerting systems for suspicious activity
- Enhancing incident response procedures and staff awareness

The case underscores the growing regulatory expectation for organisations to proactively manage data risks and ensure Privacy by Design across digital services that handle consumer information.

**Read our blog** for 5 tips on an effective data breach response.

---

# California introduces law requiring browsers to include opt-out preference signal

On 8 October 2025, California's governor signed the Opt Me Out Act (AB 566) into law, amending the California Consumer Privacy Act (CCPA) to make it easier for residents to exercise their right to stop the sale of their personal data. The law requires browser developers to include a built-in preference signal that lets users block data sales with a single setting, rather than opting out on every website.

Set to take effect on 1 January 2027, the Bill recognises that privacy rights lose meaning if exercising them is overly complex. Under the new rules, browser companies must also inform users how the opt-out signal works and will receive liability protection when a website fails to honour the preference correctly.

Businesses operating websites should ensure their systems can accurately detect and respect browser-based opt-out signals and update privacy notices to clearly explain how these preferences are handled.

**Read Assembly Bill 566**


## UNITED KINGDOM

# ICO launches consultation on charitable purpose soft opt-in

The Information Commissioner's Office's consultation focuses on new rules to the Privacy and Electronic Communications Regulations 2003 (PECR), introduced by Section 114 of the Data Use and Access Act 2025. The amendment will allow charities to send electronic mail marketing about their charitable purposes to existing supporters without prior consent, provided they meet specific conditions.

The ICO hopes feedback will help shape updates to its PECR guidance, clarifying how charities can rely on the forthcoming *charitable purpose soft opt-in* when communicating with donors and volunteers. This provision is not yet in force, but understanding its scope early will help charities prepare their systems and consent processes ahead of implementation.

**Respond to the consultation**, which is open until 27 November 2025.

## EUROPEAN UNION

# European Data Protection Board opens consultation on DMA-GDPR guidelines

The *Joint Guidelines on the Interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR)* aim to ensure consistent interpretation and coherent application of both frameworks, helping organisations navigate overlapping compliance obligations.

Focusing on 'gatekeepers' (large digital platforms that process personal data), the document clarifies how key GDPR principles interact with DMA obligations on data sharing, interoperability, and user consent. It also outlines how enforcement authorities should coordinate to prevent conflicting requirements.

Individuals and organisations can **provide feedback on the consultation**, which is open until 4 December 2025.

---

# EDPB adopts formal opinions on UK adequacy under GDPR and LED

The European Data Protection Board (EDPB) opinions recommend extending adequacy under both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) until December 2031.

The EDPB noted that most of the changes in the UK's data protection framework aim to clarify and simplify compliance. However, it also urged the European Commission to monitor certain developments closely, particularly new ministerial powers introduced under the Data Use and Access Act 2025 and rules on automated decision-making and onwards data transfers.

Organisations transferring personal data between the EU and UK should continue to rely on existing adequacy arrangements but monitor the final decisions closely. It's important to review transfer mechanisms, assess whether additional safeguards may be required once the decisions are adopted, and stay informed of ongoing monitoring by EU and UK authorities.

**Read the EDPB Opinions**

---


## INTERNATIONAL

# Australian Federal Court orders Australian Clinical Labs (ACL) to pay $5.8M in civil penalties

The decision follows a 2022 data breach that resulted in unauthorised access to the personal information of more than 223,000 individuals through ACL's Medlab Pathology business. The court found that ACL failed to:

- Take reasonable steps to protect personal information
- Conduct a proper assessment of whether an eligible data breach had occurred following a cyberattack
- Prepare and submit a breach statement to the Commissioner as soon as practicable

This marks the first civil penalty imposed under Australia's Privacy Act 1988. The case underscores growing regulatory expectations of robust data security and timely breach management, particularly for organisations handling sensitive information.

For more information on when to report a data breach, **read the Office of the Australian Information Commissioner's guides**.


## 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 (The Netherlands)**
- **Data Protection Officers (EU)**
- **Data Protection Officers - Life Sciences (United Kingdom)**
- **Data Protection Coordinator - Life Sciences (Poland)**
- **Chief Revenue Officer (United Kingdom)**
- **Marketing Content Coordinator (United Kingdom)**

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

FOLLOW US ON LinkedIn