



GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE



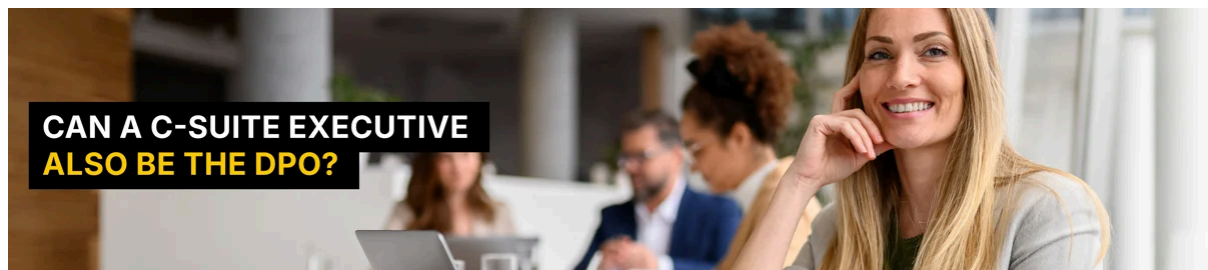
The DPOA is an assessment of the impact of the most significant and important-to-know data protection issues from around the globe. It's not the full story, just a quick 3-minute read, collated and condensed to keep you updated with the latest news in our ever-evolving industry.

Can a C-suite executive also be the DPO?

There is no outright ban on a C-suite executive acting as a Data Protection Officer (DPO) under the GDPR, but their responsibilities must not create a conflict of interest. In practice, senior leaders often make decisions about how and why personal data is processed, making it difficult for them to independently oversee those same decisions.

Our latest blog explains how to identify potential conflicts of interest, which senior roles are most likely to be incompatible with DPO responsibilities, and how to structure the role to maintain effective and independent oversight.

[Read our blog](#)



UNITED STATES & CANADA

Public Claude chats highlight risks of workplace LLM use

Hundreds of conversations shared through Anthropic's Claude AI were found to be accessible through online search engines, with some containing personal information, workplace material, and potentially confidential research. Claude chats are private by default, but users can create public links to share conversations with others.

The incident highlights the risks of employees using sharing features within generative AI tools without fully understanding who may be able to access the resulting content. Organisations should ensure AI policies and staff training clearly address what information can be entered into AI systems, as well as how outputs and conversations may be shared.

[Download our LLM White Paper](#) for practical guidance on AI governance and using LLMs responsibly.

Canada publishes Charter Statement on proposed privacy reforms

Canada's Department of Justice has published its Charter Statement on [Bill C-36](#), which would introduce the Protecting Privacy and Consumer Data Act (PPCDA) and substantially reform Canada's private-sector privacy framework. The Statement considers how the proposed legislation could affect rights and freedoms protected under the Canadian Charter.

It also provides further detail on the proposed enforcement regime, including expanded investigation and audit powers, administrative monetary penalties, and new offences for certain violations. Organisations operating in Canada should continue monitoring Bill C-36 as it progresses through Parliament and prepare for potentially stronger regulatory oversight if the reforms become law.

[Read the Charter Statement](#)

Meta agrees landmark settlement over harm to children

Meta has agreed to pay at least \$12.1 billion to settle claims brought by 51 US states and territories. The claims allege that Facebook and Instagram were designed to encourage compulsive use by children whilst misleading users and parents about the associated risks. The proposed settlement remains subject to court approval.

Alongside the financial settlement, Meta must introduce significant changes to protect younger users, including time restrictions, age assurance measures, and enhanced parental controls.

The agreement reflects growing expectations for online platforms to identify younger users and build appropriate safeguards into the design of their services.

[Learn more about the settlement](#)

PRIVACY PUZZLE WEBINAR



UNITED KINGDOM

New information access requirements for social housing providers

From 1 October 2026, private registered providers of social housing must comply with the first phase of the Social Tenant Access to Information Requirements (STAIRs). Providers must proactively publish information about how they operate and establish a policy for handling information requests.

Tenants will be able to request information about the management of their social housing from 1 April 2027, with requests generally requiring a response within 30 calendar days.

Providers should review their publication and information-handling processes now, including how staff will identify and respond to STAIRs requests alongside existing Data Subject Access Request (DSAR) and Freedom of Information (FOI) procedures.

[Learn more about STAIRs](#)

EUROPEAN UNION

Irish DPC proposes €8-11M fine against Tinder

An investigation examined the platform's handling of data access and erasure requests, with preliminary findings alleging that certain access and retention policies breached GDPR requirements. The final decision is still pending.

The case serves as a reminder that organisations should be able to justify how long personal data is retained and ensure individuals can effectively exercise their data protection rights.

[Read our blog](#) on data retention to learn best practices for compliance.

EU seeks information from AI developers as enforcement begins

The European Commission has reportedly issued requests for information to developers of some of the world's most advanced AI models as it begins exercising its enforcement powers under the EU AI Act. The requests focus on cybersecurity and safety practices, including model protection, external evaluations, and post-deployment monitoring.

As the Commission moves from implementation towards active oversight of AI Act compliance, providers of general-purpose AI models should ensure they can demonstrate how risks are identified, assessed, and mitigated.

[Read our blog](#) for essential strategies to support EU AI Act compliance.



INTERNATIONAL

China simplifies privacy compliance for small-scale data handlers

From 1 September 2026, organisations in China that process personal information relating to fewer than 100,000 individuals may benefit from simplified requirements under new Personal Information Protection Law (PIPL) measures.

Eligible organisations will be able to:

- Follow streamlined processes for Privacy Notices and consent
- Use simplified templates for privacy impact assessments
- Conduct compliance audits once every five years

Certain businesses operating solely through online platforms may also be able to rely on privacy measures implemented by the platform.

Organisations operating in China should assess whether they meet the threshold and identify where the new measures could simplify their existing compliance processes.

[Learn more about the new 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 Officer - Life Sciences (Poland)**
- **Data Protection Coordinator - Life Sciences (Poland)**

If you are looking for a new and exciting challenge, [apply today!](#)

FOLLOW US ON **LinkedIn**

Copyright © 2026 The DPO Centre, All rights reserved.

You have been sent this newsletter under legitimate interest, for more information please read our [Privacy Notice](#)

The DPO Centre is a limited company registered in England and Wales (Company Number: 10874595)

The DPO Centre Group
London | Amsterdam | Toronto | Dublin

[Unsubscribe](#) [Manage Preferences](#)