



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.

AI social engineering attacks: Protect data and stay compliant

AI is making social engineering scams faster, more convincing, and harder to detect. Criminals can scrape personal details for precision targeting, send flawless phishing emails, and even impersonate executives with deepfakes — tactics that conventional technical defences alone can't reliably stop.

Our latest blog explains how these attacks unfold and why traditional safeguards are no longer enough. It highlights the key steps organisations should take to strengthen resilience and maintain compliance in the face of AI-driven threats.

[Read our blog](#)



UNITED KINGDOM

NHS England publish DSPT version 8

On 1 September 2025, NHS England released version 8 of the Data Security and Protection Toolkit (DSPT) for 2025/26. The new version includes an updated set of Outcomes, Assertions, and Evidence items, together with a detailed change log comparing the new requirements against last year's version.

Key updates include:

- Continued alignment with the Cyber Assessment Framework (CAF) version 3.4, reinforcing an outcome-based approach rather than prescriptive controls

- Refreshed evidence items, with some clarified and others expanded
- Sector-specific updates for NHS Trusts, Integrated Care Boards, IT suppliers, pharmacies, and social care providers, set out in the change log

Organisations should review the change log early to identify where processes, policies, or technical controls need updating ahead of the new reporting year and to avoid last-minute compliance gaps. The deadline for 2025/26 DSPT submissions is 30 June 2026.

[Download the change log](#)

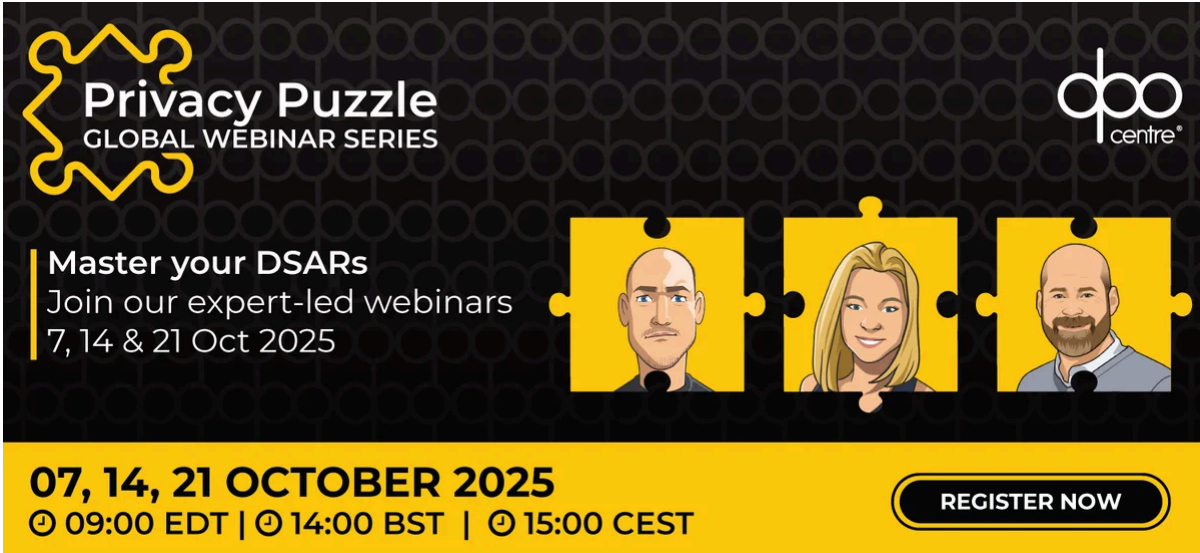
ICO fines care home director for ignoring DSAR

The Information Commissioner's Office (ICO) has fined a care home director £1,100 after he refused to respond to a Data Subject Access Request (DSAR). An investigation found the director deliberately blocked, erased, or concealed records to prevent disclosure. The withheld information included incident reports, CCTV footage, and care notes.

Under the UK General Data Protection Regulation (GDPR), individuals have the right to obtain a copy of the personal information that an organisation holds about them. Organisations must respond to DSARs within one month (extendable by two months for complex cases) and should have clear procedures to locate, review, and securely disclose the requested information within that timeframe.

Our upcoming webinar mini-series will explore the key challenges of DSAR compliance, covering the new requirements under the Data Use and Access Act (DUAA) and a dedicated focus on reducing risk in healthcare settings.

[Register for our DSAR webinar mini-series now](#)



Privacy Puzzle
GLOBAL WEBINAR SERIES

Master your DSARs
Join our expert-led webinars
7, 14 & 21 Oct 2025

07, 14, 21 OCTOBER 2025
🕒 09:00 EDT | 🕒 14:00 BST | 🕒 15:00 CEST

REGISTER NOW

EUROPEAN UNION

Google receives third CNIL fine for invalid cookie practices

On 1 September 2025, France's data protection authority (CNIL) fined Google Ireland Limited and Google LLC €325 million for breaching the French Data Protection Act and the Postal and Electronic Communications Code (CPCE).

The CNIL found that when creating a Google account, users were steered towards personalised advertising cookies, not clearly told these were a condition of accessing services, and faced greater difficulty refusing than accepting them — making consent invalid. It also ruled that Google had inserted adverts between Gmail messages without prior consent.

This is the CNIL's third major sanction against Google for cookie-related practices, following fines in 2020 and 2021.

The case highlights the need for organisations to ensure cookie consent is genuinely balanced, refusal is as simple as acceptance, and any advertising or tracking is transparent and based on freely given, informed consent.

[Read the CNIL's guidance on cookies](#)

CJEU clarifies when pseudonymised data is personal

On 4 September, the Court of Justice of the European Union (CJEU) ruled that pseudonymised data is not automatically personal data in all circumstances. Whether it falls under the General Data Protection Regulation (GDPR) depends on the recipient's ability to re-identify individuals.

This important judgement makes clear that:

- Controllers remain subject to GDPR if they retain the means to re-identify data subjects, even when sharing pseudonymised datasets with third parties
- Recipients may not be processing personal data if re-identification is genuinely impracticable without disproportionate effort
- Opinions and views are inherently personal data when linked to an identifiable person
- Transparency obligations still apply at the point of collection, and privacy notices must accurately set out all potential recipients

For organisations, the ruling is a reminder that pseudonymisation reduces risk but does not guarantee GDPR no longer applies. Each scenario requires a case-by-case assessment of identifiability and transparency.

[Read the judgement](#)

Dutch report offers tools to make GDPR practical

On 26 August 2025, the Dutch Ministry of Foreign Affairs published an advisory report on improving GDPR information for entrepreneurs. The report aims to make the Regulation more practical and easier to apply in day-to-day operations.

It introduces three concepts:

- Decision aids that translate open legal standards into real-world business scenarios
- A toolkit of success stories, highlighting benefits through shared experiences
- Guidance to debunk common GDPR misconceptions that hinder compliance

For organisations, the report serves as a reminder that the GDPR is not only about avoiding fines but can also support business growth when understood and implemented effectively.

[Read the report](#)

WE'RE SPONSORING
AI IN THE PUBLIC SECTOR CONFERENCE



**ACCELERATING AI'S ADOPTION,
IMPLEMENTATION AND ROLL-OUT**
DAVID SMITH, DPO & AI SECTOR LEAD



25 SEP 2025
LONDON, UK



CANADA & UNITED STATES

Disney to pay \$10M over alleged COPPA violations

The US Federal Trade Commission (FTC) has announced that Disney will pay \$10 million to settle allegations that it violated the Children's Online Privacy Protection Act (COPPA).

According to the FTC, Disney failed to properly label some of its YouTube videos as "Made for Kids". This mislabelling meant YouTube collected personal data from children under 13 without parental consent, using it for targeted advertising. It also exposed children to features not intended for young users, such as autoplay into non-child-directed content.

To comply with the COPPA Rule, organisations should:

- Accurately identify and label child-directed content
- Provide clear privacy notices to parents
- Obtain verifiable parental consent before collecting, using, or disclosing data from children under 13
- Avoid behavioural advertising or tracking without consent
- Ensure key features are age-appropriate

[Read the FTC COPPA guidance](#)

OPC calls for privacy clause to be restored in Canada's Broadcasting Act

On 5 September 2025, the Office of the Privacy Commissioner of Canada (OPC) wrote to the Minister of Canadian Identity and Culture, urging the federal government to reinstate a privacy clause in the recently amended Broadcasting Act.

The amendment, made through the Act for the Substantive Equality of Canada's Official Languages (formerly Bill C-13), inadvertently removed a provision requiring the Act to be "construed and applied in a manner that is consistent with the right to privacy of individuals."

The OPC described the clause as an important guiding principle and expects the government to correct the error as soon as possible. Restoring the privacy clause would reaffirm privacy as a core consideration in broadcasting and streaming regulation, signalling continued regulatory focus on how broadcasters and online platforms protect audience data.

[Read the OPC's letter](#)

INTERNATIONAL

South Korea launches 3-month crackdown on illegal data distribution

On 9 September 2025, South Korea's Personal Information Protection Commission (PIPC), together with the Korea Internet & Security Agency (KISA), announced a three-month initiative to monitor and block the illegal online distribution of personal information. The action follows a surge in hacking incidents affecting telecom and credit card companies, which has led to increased financial fraud and heightened public concern.

Monitoring will focus on websites, online communities, and social networking services where personal data is likely to be shared. The PIPC plans to rapidly delete and block posts exposing resident registration numbers, phone numbers, account or credit card details, and any content selling or purchasing databases of personal information.

The PIPC will also provide a self-checklist to help local governments and festival organisers secure temporary event websites, which are often vulnerable to data leaks. The monitoring campaign will run from September through November 2025.

[Read the PIPC press release](#)

AOB

The DPO Centre joins Axiom GRC

On 1 September 2025, The DPO Centre was acquired by [Axiom GRC](#), a leading provider of governance, risk, and compliance solutions. The move supports our plans to accelerate international growth and build on the strong client relationships we've developed since 2017.

As part of the transition, founder Rob Masson has stepped down as CEO. He is succeeded by former COO Lenitha Bishop, who will lead the business into its next phase and strengthen collaboration with Axiom GRC's network of specialist compliance companies.

[Read the full story.](#)



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 (United Kingdom)
- Data Protection Officers (The Netherlands)
- Data Protection Officers (EU)
- Data Protection Officers - Life Sciences (United Kingdom)
- Data Protection Support Officers (United Kingdom)

If you are looking for a new and exciting challenge, and the opportunity to work for a **Great Place to Work-Certified™** company, **ranked in the top 50 of the UK's Best Workplaces™ for medium-sized businesses**, [apply today!](#)



FOLLOW US ON **LinkedIn**

Copyright © 2025 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 | New York | Toronto | Dublin

