



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.

GDPR & AML: Why Financial Services must align KYC, CDD and data protection

Digital onboarding and AI-powered verification are reshaping the way Financial Services screen customers. As these processes become more data intensive, Anti Money Laundering (AML) and GDPR requirements can no longer operate in silos.

Our latest blog explains why Know Your Customer (KYC), Customer Due Diligence (CDD), and data protection need to work together. We explain where compliance blind spots typically arise and the steps firms can take to protect customers and remain compliant.

[Read our blog](#)



UNITED KINGDOM

ICO report emphasises safeguards in HealthTech AI

On 14 November 2025, the Information Commissioner's Office (ICO) published its exit report on the Visual Intelligence project — an AI-enabled falls-prevention system developed by Eclipse Digital Solutions and Geutebruck UK for use in health and social care settings.

The report emphasises the need to:

- Clearly establish data protection roles (controller, joint controller, processor)
- Document necessity and proportionality assessments for sensitive health data
- Embed Privacy by Design from the earliest development stage

It also encourages organisations developing AI, Internet of Things, or sensor-based solutions to review their Data Protection Impact Assessment (DPIA) workflows, map roles clearly, and ensure proportionate safeguards when monitoring vulnerable people or handling health data.

[Read the report](#)

UK High Court largely rejects copyright claim against Stability AI

Getty Images launched the lawsuit after alleging that Stability AI had scraped millions of its copyrighted photographs without permission to train its image-generation model, Stable Diffusion.


The Court found that Stable Diffusion does not store or reproduce Getty's images in the model weights, so the software is not an 'infringing copy' under UK law. Since the key training activity occurred outside the UK, most copyright claims were dismissed. However, some trademark issues remain after the model generated images showing Getty's watermark.

The ruling suggests that training a model on copyrighted works may not automatically infringe rights if those works are not retained in the model.

Whilst it offers useful guidance, it doesn't settle the issue worldwide. Organisations should still check that their training data and licences are robust, especially where other legal frameworks may take a different view.


[Read our blog](#) to explore how AI Impact Assessments (AIAs) support responsible model development.


ONLINE WEBINAR





Privacy Puzzle
GLOBAL WEBINAR SERIES
27 NOV 2025


DOUBLE BLIND: Secondary use of health data and AI in clinical trials








Ben Seretny





Lawrence Carter




Pippa Scotcher




Michael McCagh


EUROPEAN UNION

European Commission unveils Digital Omnibus

On 19 November 2025, the [Digital Omnibus](#) package was officially announced. This wide-reaching proposal is designed to streamline EU regulation and reduce the administrative burden for businesses.

Key proposed reforms include:

- Updates to the General Data Protection Regulation (GDPR)
- Targeted amendments to the EU AI Act
- Modernised cookie rules to improve user experience
- Improved access to data via the Data Act by merging four existing pieces of legislation into one

The release has sparked much debate across the EU with some viewing it as a necessary evolution of the GDPR, and others warning it may dilute long-standing protections.

[Read our initial analysis here](#), with early insights from our Data Protection Officers.

EU adopts faster cross-border complaint process

On 17 November 2025, the Council of the European Union adopted new rules to streamline how national data protection authorities deal with cross-border complaints under the General Data Protection Regulation (GDPR).

The changes will:

- **Harmonise admissibility** criteria so all Member States assess complaints on the same basis
- **Standardise rights** for complainants and organisations under investigation
- **Introduce deadlines** for investigations to be concluded within 15 months (or 12 months for simplified cases)
- **Enable simpler cooperation procedures** for straightforward cases, allowing authorities to settle investigations without triggering the full cooperation mechanism

The regulation enters into force 20 days after publication in the Official Journal and will apply 15 months thereafter. Organisations with cross-border processing should review governance structures, reduce bottlenecks in regulatory engagement, and ensure their documentation can withstand increased scrutiny.

[Learn more](#)

Dutch regulator publishes feedback on AI social scoring ban

It follows the data protection authority's call for input on the EU AI Act's prohibition of social scoring systems, during which organisations raised concerns about how the rules will apply in practice. Published on 14 November 2025, Autoriteit Persoonsgegevens (AP) highlighted two key concerns for organisations:

- **Risk of discrimination and chilling effects:** Individuals may change behaviour to avoid negative scores, affecting autonomy, freedom of expression, and social justice
- **Lack of clarity in the law:** Organisations need clearer guidance on concepts like social behaviour, evaluation vs classification, and when treatment is disproportionate or occurs in an unrelated context

The AP will use these insights to support supervisory preparation in the Netherlands and contribute to future EU guidance on prohibited AI practices.

Organisations should review any AI models that score individuals and be prepared to evidence safeguards against discrimination and disproportionate impacts.

[Read the summary](#)



CANADA & UNITED STATES

Ontario's IPC publishes updated guide to Privacy Impact Assessments (PIAs)

Released on 12 November 2025, the guide is designed to help institutions subject to the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) conduct mandatory PIAs.

It introduces a four-step methodology and outlines the required elements of a PIA, including the purpose and legal authority for collection, categories of personal information, retention periods, and the safeguards in place to reduce privacy risks.

Organisations operating under FIPPA, and by good practice MFIPPA, should now adopt the new methodology and check that their PIA templates include all mandatory information.

[Download the guide](#)

New York AI Companion Models Act enters into effect

From 5 November 2025, the Act imposes new duties on systems designed to simulate social interaction. AI companions may retain personal details, tailor responses to user preferences, and encourage continued interaction.

Providers must now:

- Clearly disclose the interaction is with AI and provide reminders every three hours of sustained use
- Detect and respond to signs of self-harm or suicidal ideation, directing users to crisis-support services
- Maintain safeguards to prevent psychological manipulation or exploitation

Enforcement falls to the New York Attorney General, with civil penalties up to \$15,000 per day for violations.

With companion-style AI tools gaining rapid adoption among young and vulnerable users, organisations should ensure these protections are built-in and documented from the outset, not retrofitted after launch.

[Read the Act](#)

INTERNATIONAL

Singapore introduces Health Information Bill (HIB) to Parliament

The Bill aims to overhaul how healthcare providers process and share patient health data via the National Electronic Health Record (NEHR) system. Under the Bill, all healthcare service providers licensed under the Healthcare Services Act (HSA) or authorised by the Ministry of Health (MoH) must:

- Contribute data to the NEHR
- Implement measures to protect patients' health information, including timely updates to systems and software
- Ensure staff are equipped to safeguard cybersecurity
- Report cybersecurity incidents and data breaches
- Store, reproduce, and transmit data in line with the Bill's requirements

Organisations should now review their data governance frameworks to check alignment with these requirements, clarify roles for contribution and access, and reassess any third-party arrangements or cross-border analytics that may fall under increased regulatory scrutiny.

[Learn more about the HIB](#)



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 Coordinator - Life Sciences (Poland)**
- **Chief Revenue Officer (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

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