



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.

---

## Large-scale processing and the GDPR: When to appoint a DPO

For North American companies handling EU personal data, understanding what qualifies as large-scale processing is essential – it could be the deciding factor in whether you need to appoint a Data Protection Officer (DPO) under the GDPR. But what qualifies as 'large-scale'?

In our latest blog, we break down what 'large-scale' really means and offer practical examples from key sectors to help you assess your obligations.

[Read our blog](#)



---

**CANADA & UNITED STATES**

## Ontario health agency under scrutiny for delayed breach notifications

Ontario Health atHome is facing criticism over delays in notifying the Information and Privacy Commissioner (IPC) of Ontario and affected patients after a major cyberattack. The organisation discovered the breach on 14 April 2025, which exposed the personal information of up to 200,000 patients, including names, contact details, and records of ordered medical supplies. They didn't notify the IPC until 30 May and waited until 27 June to begin informing patients.

Under Ontario's Personal Health Information Protection Act (PHIPA), organisations must notify the IPC and affected individuals 'at the first reasonable opportunity' if personal

health information is compromised.

The IPC has published [Guidelines for the Health Sector](#), containing practical breach management advice and compliance requirements.

---

## The White House publishes controversial AI Action Plan

On 23 July 2025, the Trump administration unveiled [Winning the Race: America's AI Action Plan](#), a national strategy aimed at securing US dominance in artificial intelligence.

The plan outlines over 90 federal actions across three pillars:

1. Accelerating innovation
2. Building American AI infrastructure
3. Leading in international diplomacy and security

The plan focuses on deregulation, open-source development, and AI exports, while limiting funding for states with stricter AI laws — representing a clear shift from the previous focus on civil rights, transparency, and algorithmic risk mitigation.

[Read our latest article](#) for early perspectives from our AI Sector Lead on the new US strategy, with practical takeaways for organisations navigating transatlantic AI regulation.

---

## Clorox files \$380M lawsuit against IT vendor following major breach

On 23 July 2025, Clorox filed a lawsuit against its IT service provider, Cognizant, alleging that weak identity checks led to a major cyberattack in 2023. The breach allegedly began when a hacker impersonated Clorox employees over the phone and was granted password and MFA resets without proper checks.

Clorox says Cognizant repeatedly assured them that support agents were following agreed protocols, but the cybercriminal was able to access the network and escalate privileges across multiple accounts. This resulted in weeks of disruption and losses totalling \$380 million.

The case highlights the need for strong internal governance, vendor oversight, and staff training. Organisations must ensure that third-party helpdesks enforce robust identity checks and log all access requests, particularly those involving credentials or MFA.

For practical steps on assessing vendor risks, read our blog on [GDPR-compliant vendor due diligence](#).

---

WE'RE **ATTENDING**

MARCUS EVANS EVOLUTION SUMMIT



evolution  
summit

a **marcusevans** event

11-13 SEP 25  
SAN DIEGO, CA

## UNITED KINGDOM

### UK to regulate police use of facial recognition technology

The UK Home Office has confirmed plans to introduce a legal governance framework for law enforcement's use of facial recognition technology. The government is working closely with police forces to develop clear standards for deployment, aiming to address growing concerns over unchecked expansion of the technology.

The move follows repeated calls from Parliament and civil society for statutory regulation, amid fears that facial recognition is being adopted by police without adequate scrutiny, transparency, or oversight. Critics have warned that the current patchwork of guidance and case law is insufficient to protect individual rights.

By establishing a clear legal basis and oversight structure, the Home Office hopes to provide both accountability and assurance, helping police forces adopt facial recognition responsibly while maintaining public trust.

[Watch our on-demand webinar](#) on Live Facial Recognition to gain innovative solutions for successful deployment of LFR technologies.

## EUROPEAN UNION

### CNIL opens consultation on web filtering gateway recommendation

On 28 July 2025, the French Data Protection Authority (CNIL) launched a public consultation on a draft recommendation regarding the use of web filtering gateways. These tools are commonly used by organisations to monitor or block employee access to certain online content, often for cybersecurity or productivity purposes.

The recommendation aims to provide legal certainty to data controllers using these solutions while encouraging service providers to adopt a Privacy by Design approach in line with GDPR principles. It applies to organisations deploying network-level filtering systems that manage web access for employees, service providers, or external visitors using their networks.

[View the draft recommendation](#) and [take part in the consultation](#), which is open until 30 September 2025.

---

## European Commission unveils transparency template for GPAI

On 24 July 2025, the European Commission published a standardised template to help general-purpose AI (GPAI) providers comply with transparency obligations under the EU AI Act. From 2 August 2025, newly placed GPAI models must include a summary of the training data used, while existing models have until 2027 to meet the same requirement.

Designed to support consistent and structured disclosures, the template balances transparency with commercial confidentiality. Key fields include:

- Provider and model identification
- Types and volume of training data
- Data sources
- Measures to exclude unlawful or biased data
- Steps to safeguard copyright and trade secrets

Non-compliance may result in penalties up to €15 million or 3% of global turnover. Providers are encouraged to adopt the template early to prepare for forthcoming regulatory expectations.

[Download the template](#)

---



**WE'RE ATTENDING**

**COG: CRO SUMMIT EUROPE 2025**

**16-17 SEP 25**  
**AMSTERDAM, NL**

**Clinical Outsourcing Group**  
**CRO Summit Europe**

doo  
centre



## China launches new DPO registration portal

The Cyberspace Administration of China (CAC) has launched a new online portal for registering Data Protection Officers (DPOs), marking a significant administrative change under China's Personal Information Protection Law (PIPL).

Registering a DPO has long been mandatory, but the portal now provides a formal mechanism for organisations that process the personal data of 1 million or more individuals to submit required details to the regulator.

Organisations must provide the DPO's contact information, as well as details about their processing activities. This includes (but is not limited to) the categories of personal data handled, the number of monthly data subjects, and any cross-border transfers. Importantly, overseas organisations are also in scope if they process personal data of individuals in China.

Data controllers that already meet the requirements have until the 29 August 2025 to register their DPO, while organisations meeting the 1M threshold after the 18 July have 30 working days to submit their reports.

### [Register your DPO](#)



**LOOKING  
FOR A  
GREAT  
PLACE  
TO WORK?**

**JOIN US**

**dpo**  
centre

## 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/The Netherlands/EU)**
- **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**

---

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](#)