



WERELDWIJD PRIVACYNIEUWS  
VAN DPO CENTRE



**The DPIA** is een beoordeling van de impact van de belangrijkste en bekendste kwesties op het gebied van gegevensbescherming uit de hele wereld. Het is niet het volledige verhaal, maar slechts een snelle samenvatting van 3 minuten, verzameld en samengevat om u op de hoogte te houden van het laatste nieuws in onze steeds veranderende branche.

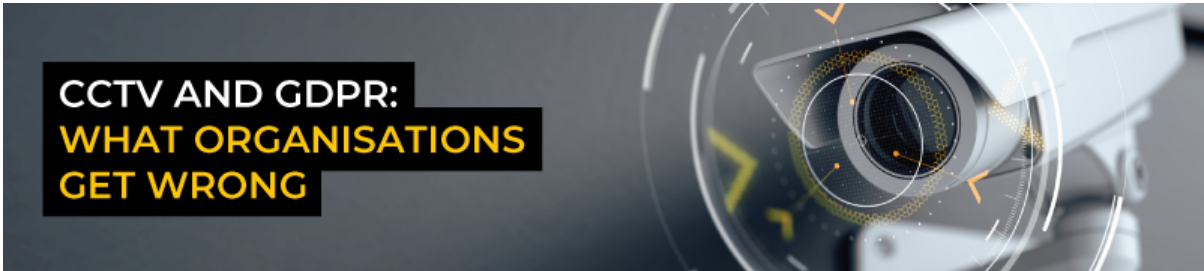
---

## CCTV and GDPR: What organisations get wrong

Our latest blog explores the most frequent mistakes organisations make when using CCTV at work and how to stay GDPR compliant. As CCTV footage can be considered personal data, it is essential to handle it lawfully and transparently.

We take a look at seven key areas for compliance, including choosing a valid lawful basis, assessing necessity and proportionality, conducting DPIAs, and how to clearly inform staff and visitors. The blog also covers best practices for access control, having a robust CCTV policy, and lawful sharing of footage.

A must-read for any organisation using workplace surveillance - [Read the full blog](#)



**CCTV AND GDPR:  
WHAT ORGANISATIONS  
GET WRONG**

---

**EUROPEAN UNION**

## Landmark EU ruling on advertising consent pop-ups

On 14 May 2025 the Belgian Court of Appeal ruled that the Transparency and Consent Framework (TCF), developed by the Interactive Advertising Bureau (IAB) Europe and used by Google, Amazon, Microsoft, and much of the online AdTech industry, is illegal under the GDPR.

The TCF system relies on pop-up windows, asking users to agree to the use of cookies and other tracking technologies. The Court found this method of collecting and processing user preferences doesn't meet the GDPR's requirements for informed consent. This ruling upholds the Belgian Data Protection Authority's 2022 findings that the TCF fails to secure personal data, lacks valid consent mechanisms, and does not provide transparency.

The decision applies immediately and signals a major shift for tracking-based advertising across Europe. Companies will now have to find alternative ways to obtain consent for tracking.

Need a refresher on GDPR-compliant lead generation? [Read our blog](#)

---

## EU confidence in EU-US data transfer mechanism falters

The EU-US Data Privacy Framework (DPF), adopted in July 2023, was intended to restore stability for data transfers between the EU and US. It followed the collapse of Safe Harbour and Privacy Shield frameworks, both invalidated by the Court of Justice of the EU over concerns about US surveillance laws.

On 5 May 2025, a report highlighted President Trump's dismissal of three Privacy & Civil Liberties Oversight Board members and a new Executive Order 14215, which brings Federal Trade Commission enforcement under White House review. These moves undermine safeguards the EU relied on.

EU reaction has been swift, with Norway's Datatilsynet and other Data Protection Authorities urging businesses to prepare 'exit strategies'. The European Data Protection Board (EDPB) has also raised adequacy concerns, and Max Schrems warns the DPF may fall without even needing a formal challenge.

### Advice for businesses

Keep your DPF certification active but explore alternative arrangements. Where applicable, assess if Standard Contractual Clauses (SCCs) apply to US transfers, and estimate the time and effort needed to roll these out at speed.

---

## Dutch DPA Targets Misleading Cookie Banners

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) will audit 500 organisations annually over the next few years to tackle misleading cookie banners.

Announced on 30 April 2025, this initiative follows earlier investigations revealing widespread non-compliance with GDPR cookie consent rules. The AP has already warned the first 50 companies. Key violations include pre-ticked boxes, hard-to-refuse options, and unclear consent requests. In response, the AP published nine rules for lawful cookie banner design. Organisations failing to comply within three months risk formal investigation and fines. The AP's focus spans both large and small organisations across all sectors.

[Read the 9 rules for clear cookie banners](#)

---

WE'RE **ATTENDING**

BIO INTERNATIONAL CONVENTION 2025



16-19 JUN 25  
BOSTON, MA

International  
Convention

UNITED KINGDOM

## UK plans data-driven surveillance of migrants

The UK government's new immigration white paper, published on 12 May 2025, proposes using eVisa data, AI, and biometric technologies to monitor migrants and help tighten border control. The system aims to track status changes, restrict access to services and support immigration raids. Critics warn this could deepen mistrust, cause errors, and lead to human rights abuses, especially given ongoing eVisa system failures.

Civil rights groups call the approach discriminatory, while the tech sector warns it risks deterring global talent and undermining the UK's ambitions in AI and innovation.

[Read the immigration white paper](#)

## ONLINE WEBINAR

### EXPANDING TRIALS INTO EUROPE



WEBINAR **marcus evans** online events

**EXPANDING TRIALS INTO EUROPE:**  
OVERCOMING DATA PRIVACY  
HURDLES IN CLINICAL RESEARCH

25 JUN 25  
ONLINE

TIME  
12PM ET | 9AM PT

**ROB MASSON**  
FOUNDER AND CEO  
THE DPO CENTRE GROUP

## CANADA & UNITED STATES

### US House passes AI moratorium amid rising opposition

On 22 May, the US House of Representatives passed the 'One Big Beautiful Bill Act', which contains a 10-year suspension on state-level AI regulation.

Despite fierce opposition and a letter to Congress from over 100 organisations, including Georgetown Law and the Alphabet Workers Union, the bill now advances to the Senate.

Critics say it undermines state laws tackling algorithmic bias and deepfakes, while the White House argues deregulation supports innovation. With AI increasingly shaping decisions in hiring, healthcare, and policing, the debate highlights growing tensions between enabling technological progress and ensuring responsible oversight.

[Track the bill's progress](#)

### US tops global data breach cost despite signs of progress

According to the Ponemon Institute's Cost of a Data Breach Report for 2024, the average cost of a data breach in the US was \$9.36 million, the highest globally for the 14th consecutive year.

While slightly lower than 2023's \$9.48 million, the US still outpaced other regions, with Healthcare remaining the most expensive industry, averaging \$9.77M per breach. The most common type of stolen data was customer and employee personal information, including tax ID numbers, emails, and home addresses. The study also found that 55% of the breaches were caused by malicious actors, while 45% were due to IT failure or human error.

With breach costs rising globally, this annual report offers a timely lens into the financial risks shaping vendor contracts, regulatory strategies and resilience planning.

[Read the 2024 breach report](#)

## INTERNATIONAL

### Malaysia issues cross-border data transfer guidelines

On 29 April 2025, Malaysia's Personal Data Protection Commissioner released the *Personal Data Protection Guideline on Cross Border Personal Data Transfers*. The guideline outlines the responsibilities of data controllers when transferring personal data outside Malaysia.

Key requirements include conducting Transfer Impact Assessments to evaluate if the destination country has similar laws to the Personal Data Protection Act 2010 (PDPA). Also, the specific conditions under which consent can be obtained and the necessity of contract for data transfers.

Organisations handling personal data in Malaysia should review data transfer mechanisms to ensure compliance with the updated requirements.

[Read the guidelines \(in Malay\).](#)



**OP ZOEK  
NAAR EEN  
FANTASTISCHE  
PLEK OM TE  
WERKEN?**

**KLIK HIER**

**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 (The Netherlands)**
- **Data Protection Officers (United Kingdom)**
- **Data Protection Officers (EU)**
- **Data Protection Officers - Life Sciences (United Kingdom/Europe/Canada)**
- **Data Protection Support Officers (United Kingdom)**
- **Data Protection Managers (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

[Manage preferences](#)