



WERELDWIJD PRIVACYNIEUWS
VAN DPO CENTRE



The DPOA 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.

Navigating international data transfers: TIAs vs TRAs

Transferring personal data internationally is critical for global businesses, but ensuring compliance can be complex, especially if you are dealing with multiple jurisdictions. Transfer Impact Assessments (TIAs) and Transfer Risk Assessments (TRAs) are essential tools to mitigate risks, but their specific requirements, timing, and methodologies can often create confusion.

In our latest blog, Katrina Leach, DPO and Head of Data Protection Operations at The DPO Centre, demystifies the distinctions between TIAs and TRAs, offering practical insights into when and how to conduct them.

[Read our latest blog](#)

EUROPEAN UNION

Irish court clarifies ownership of personal data on work devices

On 3 April 2025, the Irish High Court confirmed that personal data stored on an employer-issued device belongs to the employer - not the employee. The case involved a fire prevention officer employed by the Health Service Executive (HSE) who had used his work phone for personal matters, including accessing private email and cryptocurrency accounts. Following a cyberattack on the HSE, the employee's personal accounts were compromised, prompting him to seek compensation.

The court found that, since the employee's personal use of the phone was unauthorised and violated the HSE's acceptable use policy, the HSE was not responsible as the data controller for any personal data stored on the device.

For senior leaders and C-suite executives, this case serves as a reminder of the critical role they play in establishing and enforcing clear data protection policies within

organisations. Understanding the legal obligations and potential liabilities associated with data handling is essential. To learn more, read our blog: [Understanding data protection liabilities for C-suite executives and senior leaders](#).

EC fines Apple and Meta €700M for breaching the DMA

On 23 April 2025, the European Commission imposed fines on Apple and Meta for breaching the Digital Markets Act (DMA), marking the first enforcement actions under the new regulation.

Apple was fined €500 million for restricting app developers from informing users about alternative purchasing options outside the App Store, violating the DMA's anti-steering provisions. Meta received a €200 million fine for its 'Consent or Pay' model, which failed to offer users a genuine choice regarding the use of their personal data for personalised advertising and didn't let them freely consent to how their data was combined.

In April 2024, the European Data Protection Board (EDPB) issued Opinion 08/2024, focusing on the validity of consent in the context of 'Consent or Pay' models implemented by large online platforms. The EDPB concluded that, in most cases, these models do not meet the requirements for valid consent under the GDPR and emphasised the need for an 'equivalent alternative' that does not involve payment or extensive personal data processing.

[Read Opinion 08/2024](#)

Netherlands proposes mandatory publication of data protection fines

On 11 April 2025, the Dutch government introduced a Bill requiring the country's data protection authority, Autoriteit Persoonsgegevens (AP), to publish all fines imposed for violations of data protection laws. This move aims to enhance transparency and strengthen public trust in data privacy enforcement.

Under the proposed legislation, the AP would be obligated to disclose details of all administrative fines, including the nature of the violation and the identity of the offending party. Currently, the AP has discretion over the publication of such information.

The bill includes several exemptions to protect individuals and ongoing investigations. The AP may withhold publication if the information could identify a natural person and cause disproportionate harm, if it would unduly damage the parties involved, if it risks undermining an ongoing investigation, or if disclosure conflicts with the objectives of the GDPR Implementation Act.

If enacted, this measure would align the Netherlands with a growing trend among EU Member States to increase the visibility of data protection enforcement actions.

[Read the Bill](#)

WE'RE ATTENDING

PRIVACY SYMPOSIUM

Conference in Venice, Italy
12-16 May 2025

REGISTER



BEN SERETNY
HEAD OF DPO SERVICE



15 MAY 2025
VENICE, ITALY



UNITED KINGDOM

UK and Japan expand scope of adequacy agreement

On 23 April 2025, the United Kingdom and Japan signed a joint statement to expand the scope of their existing data adequacy agreement. Beyond commercial transfers, the updated framework extends protections to academia and the public sector, enhancing the free flow of personal data between the two countries. It also aims to facilitate collaborative research and administrative cooperation between the UK's Department for Science, Innovation and Technology (DSIT) and Japan's Personal Information Protection Commission (PPC).

The agreement builds on the UK–Japan Digital Partnership and reflects a growing alignment on digital priorities, such as infrastructure, artificial intelligence, and cybersecurity.

[Learn more about the UK-Japan Digital Partnership](#)

WE'RE ATTENDING

**Encore Boston
Harbor**

Boston, MA

**19 -
20**

May 2025
marcusevans

**Evolution
Summit**



19 - 20 MAY 2025
BOSTON, MA



CANADA & UNITED STATES

US Congress passes TAKE IT DOWN Act to combat deepfakes

On 28 April 2025, the US House of Representatives passed the bipartisan TAKE IT DOWN Act, which aims to combat the spread of non-consensual intimate images (NCII). The legislation criminalises the publication of NCII, including AI-generated deepfakes, and mandates that online platforms remove such content within 48 hours of a valid request.

The Act grants the Federal Trade Commission powers to impose fines on organisations that fail to comply with their new obligations, whilst offending individuals could face up to two years' imprisonment for offenses involving adults and up to three years for those involving minors.

The legislation marks a significant step in addressing digital exploitation and protecting individuals' privacy rights in the digital age.

[Read the TAKE IT DOWN Act](#)

CPPA sign declaration of cooperation with UK's ICO

On 29 April 2025, the California Privacy Protection Agency (CPPA) and the UK's Information Commissioner's Office (ICO) signed a declaration of cooperation to enhance privacy protections across jurisdictions. As part of the agreement, both authorities will support joint research, share best practices and investigative methods, hold staff-level meetings, and develop tools for ongoing collaboration.

This is the latest in a growing list of international partnerships for the CPPA, following similar agreements with South Korea and France. For organisations operating in both the

UK and California, this cooperation could help streamline compliance across jurisdictions in the future.

[Read the CPPA's press release](#)

INTERNATIONAL

China introduces new Measures for personal information audits

On 1 May 2025, the Cyberspace Administration of China (CAC) brought into effect 'Administrative Measures for Personal Information Protection Compliance Audits'. These new rules require personal information protection compliance audits for certain organisations under the Personal Information Protection Law (PIPL).

Key provisions:

- **Mandatory audits** for organisations processing data on over 10 million individuals, at least every two years
- **Regulator-triggered audits** may apply in cases of high-risk or major incidents
- **Audit scope** includes data handling practices, security measures, cross-border transfers, and breach response
- **DPOs required** for organisations handling over 1 million individuals' data
- **Audit reports** must be submitted to authorities, with timely remediation of any issues

These Measures significantly increase regulatory expectations for businesses operating in China and highlight the growing global trend toward mandatory privacy audits.

[Read the Measures](#)



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

KLIK HIER



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 - Life Sciences (United Kingdom/Europe/Canada)**
- **Data Privacy Officers (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](#)