



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.

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](#)

UNITED KINGDOM

ICO publishes guidance on data sharing for fraud prevention

On 22 November 2024, the Information Commissioner's Office (ICO) published guidance for organisations on sharing personal information to combat fraud. The guidance clarifies that data protection regulations do not prevent organisations from sharing personal information for legitimate purposes, such as fraud prevention. However, organisations should take additional steps to ensure compliance with their data protection obligations when doing so.

The steps include:

- Conducting a Data Protection Impact Assessment (DPIA)
- Establishing clear responsibilities for separate or joint data controllers
- Implementing data sharing agreements
- Identifying a valid lawful basis for sharing personal information

[Read the ICO's guidance](#)

UK's DUA Bill passes second reading in Parliament

On 19 November 2024, the Data (Use and Access) Bill took another step forward, passing its second reading in the House of Lords. The Bill, which aims to enhance data protection practices across businesses and services in both the public and private sectors, has received largely positive feedback so far.

However, the debate highlighted several concerns raised by lawmakers, including:

- Lack of provisions relating to AI, such as data scraping
- Proposed relaxation of restrictions on automated decision-making
- Independence of the new Information Commission from ministerial interference
- Potential abuse of 'scientific research' exemptions

In our recent article, Lawrence Carter, DPO and Life Sciences Sector Lead, shares his initial thoughts regarding the business implications of the DUA Bill.

[Read Lawrence's insights](#)

The image shows a white paper titled 'HANDLING DATA SUBJECT ACCESS REQUESTS (DSARs)' with the dpo centre logo. It is placed on a yellow background with a pattern of white circles. Other documents are visible behind it, including one with '6. IDENTIFY THE REQUEST' and another with 'APPENDIX CHECK'.

White paper: Handling Data Subject Access Requests (DSARs)

Data Subjects have the right to know if your organisation is processing their personal data, and provided with a copy of such personal data.

[READ MORE](#)

The logo for dpo centre, consisting of the letters 'dpo' in a stylized font with 'centre' written below it.

EUROPEAN UNION

Privacy group noyb granted Qualified Entity status

The privacy advocacy group, *noyb* (None of Your Business), founded by Max Schrems in 2018, has been approved as a 'Qualified Entity' (QE) to bring collective redress actions across the European Union. Under the Directive (EU) 2020/1828, *noyb* can prohibit organisations from engaging in illegal practices and file class action lawsuits on behalf of consumers for data protection violations.

This development is a significant step forward in consumer protection. With the ability to initiate collective actions, *noyb* can more effectively hold companies accountable for GDPR violations, leading to better enforcement of data protection laws and greater compliance from companies to avoid large-scale financial penalties.

[Read Max Schrem's statement and more about noyb's QE status](#)

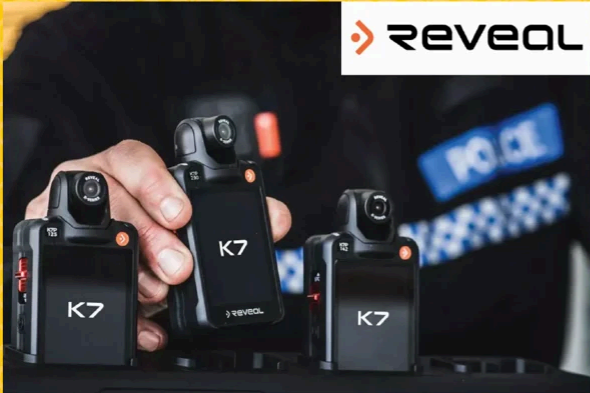
WhatsApp takes €225M GDPR battle to CJEU

On 26 November 2024, WhatsApp appealed to the Court of Justice of the European Union (CJEU) against a €225 million fine issued by Ireland's Data Protection Commission (DPC).

The fine was initially issued in 2021 for privacy breaches but was increased following an investigation by the European Data Protection Board (EDPB), which found a lack of transparency in how WhatsApp shared personal information.

To ensure transparency, organisations must present information in a concise and easily accessible way, using clear and plain language. This information must be provided in writing and free of charge.


[Read the EDPB's guidance on transparency.](#)

A hand holding three black Reveal Media K7 devices. The background is a blurred image of a police officer in a blue uniform with 'POLICE' written on the back. The Reveal logo is in the top right corner of the image.

Find out how Reveal Media solved these data protection challenges:

- Managing large volumes of data
- Ensuring data minimisation
- Providing transparent information

[READ MORE](#)

The logo for the Data Protection Officer (DPO) Centre, featuring a stylized 'dpo' and the word 'centre'.

NORTH AMERICA

FTC takes action against false FRT claims

On 3 December 2024, the Federal Trade Commission (FTC) issued a proposed consent order against IntelliVision Technologies Corp. for making false claims about its facial recognition technology (FRT). An FTC investigation found IntelliVision had misled consumers on how the FRT was trained, its accuracy, and performance.

The proposed consent order will prohibit IntelliVision from making misrepresentations about:

- The accuracy or efficacy of its FRT
- The comparative performance of the technology with respect to individuals of different genders, ethnicities, and skin tones
- The accuracy or efficacy of the technology to detect spoofing

Our recent webinar, [On face value: Understanding the privacy risks of Live Facial Recognition \(LFR\)](#), examines the challenges of implementing FRT and explores some of the innovative solutions for successful deployment.

Ontario's Bill 194 receives Royal Assent

On 25 November 2024, the Strengthening Cyber Security and Building Trust in the Public Sector Act (2024) received Royal Assent at the Legislative Assembly in Ontario. Also known as Bill 194, it creates new obligations for Ontario's public sector entities regarding privacy, cyber security, and the use of artificial intelligence.

Under Bill 194, organisations will need to:

- Develop and implement cyber security programmes
- Establish accountability frameworks when using AI systems
- Publish transparent information about their use of digital technologies and AI systems
- Notify the Commissioner and affected individuals of any data breaches, alongside an annual report
- Conduct privacy impact assessments before collecting personal information

[Read the Bill](#)

INTERNATIONAL

Australia passes Privacy and Other Legislation Amendment Bill 2024

On 29 November 2024, the Australian Government passed the Privacy and Other Legislation Amendment Bill 2024. The Bill aims to significantly strengthen Australian privacy laws and be adaptable to technological advancements.

Key provisions include:

- Requirement for transparency around automated decision-making in company privacy policies
- Greater enforcement powers for the OAIC, alongside civil penalties for privacy breaches
- Statutory tort for serious invasions of privacy
- Development of the Children's Online Privacy Code to enhance privacy protections for children in online environments
- Criminalisation of doxxing (releasing personal data without consent)

[Learn more about the Bill](#)



LOOKING FOR A GREAT PLACE TO WORK?

JOIN US

Great Place To Work®
Certified
JUN 2024-JUN 2025
UK

Best Workplaces™
for Women
Great Place To Work®
UK
2024

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)**
- **Data Protection Officer - Life Sciences (United Kingdom/The Netherlands)**
- **Data Protection Officers (The Netherlands)**
- **Data Privacy Officers (Canada)**
- **Data Protection Support Officers (United Kingdom)**
- **Copywriter (United Kingdom)**
- **Partnerships Account Manager (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, one of the UK's **Best Workplaces for Women** and **Best Workplaces in Consulting & Professional Services**, [**apply today!**](#)

FOLLOW US ON **LinkedIn**

Copyright © 2024 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, Amsterdam, Dublin, London, Toronto

[Manage preferences](#)