



GLOBAL PRIVACY NEWS
FROM THE DPO CENTRE

The DPOIA 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.

Quebec's Law 25: A guide to support compliance

Explore Quebec's new privacy legislation: Law 25. The law applies to all organisations, located anywhere, that collect, process, and store the personal information of Quebec individuals and marks a complete overhaul of Quebec's privacy regime.

We discuss its key elements and provide a guide towards compliance with the final stage of the legislation, which came into effect on 22 September 2024.

[Read our blog here](#)

CANADA & NORTH AMERICA

Bill C-65 lacks 'basic elements', says Canadian Privacy Commissioner

The Privacy Commissioner of Canada, Philippe Dufresne, has submitted feedback on the Electoral Participation Act, stating it could be improved to better secure electors' personal information. The Act, also known as Bill C-65, is a proposed legislation aimed at amending the Canada Elections Act.

Bill C-65 will introduce new requirements for political parties to protect personal information. But Dufresne said it lacks certain statutory requirements, such as seeking consent or permitting individuals to exercise a right of correction.

He provided 3 recommendations on the Bill:

- Require political parties to seek consent, limit collection, use, and disclosure of data, and provide a mechanism for access and correction
- Broaden the privacy breach notification provisions to include mandatory reporting
- Allow for formal collaboration between the Office of the Privacy Commissioner of Canada, Elections Canada, and the Commissioner of Canada Elections

[Read Dufresne's submission](#)

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](#)



DO YOU PROCESS PERSONAL DATA OF EU/UK RESIDENTS?

Our Fractional Privacy Officers bring peace of mind, helping you reduce risk.

- ✓ Comply with GDPR Article 27 and avoid data protection violations
- ✓ Reduce exposure to privacy risks
- ✓ Showcase your company's dedication to privacy rights

FIND OUT MORE

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](#)

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](#)



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



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 Privacy Officers (Canada)**
- **Data Protection Officers (United Kingdom)**
- **Data Protection Officer - Life Sciences (United Kingdom/The Netherlands)**
- **Data Protection Officers (The Netherlands)**
- **Data Protection Support Officers (United Kingdom)**
- **Copywriter (United Kingdom)**
- **Partnerships Account Manager (United Kingdom)**

If you are looking for a new and exciting challenge, [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](#)