the dpia

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.

5 steps for GDPR-compliant vendor due diligence

The global outsourcing sector continues to grow, supporting organisations with critical functions like IT and data protection. But when EU or UK personal data is shared with vendors or third parties, it's essential to understand the legal responsibilities involved.

In our latest blog, we outline five essential steps to help North American organisations conduct GDPR-compliant vendor due diligence. Whether onboarding new suppliers or auditing existing ones, the guide offers practical advice to safeguard data and meet regulatory obligations.

Read our blog

CANADA & UNITED STATES

Canada introduces Bill C-8 to enhance national cybersecurity protections

On 18 June 2025, the Canadian government introduced and passed the first reading of Bill C-8, aiming to strengthen national cybersecurity. The Bill has two main components: amendments to the Telecommunications Act and the creation of a new Critical Cyber Systems Protection Act.

The proposed legislation seeks to protect critical services and systems that are vital to national security or public safety from cybersecurity risks.

Key provisions include:

- **Expanded powers** under the Telecommunications Act, allowing the Minister of Industry to direct telecom providers to take or avoid specific actions to protect national infrastructure
- **Definition of 'critical cyber systems'**, including those whose failure could impact vital services
- **Mandatory cybersecurity programmes** for designated operators, which must address supply chain and third-party risks, detect and minimise cyber incidents, and be reviewed regularly and confirmed in writing to regulators within 90 days of designation
- **Incident reporting duties**, requiring designated operators to report cybersecurity incidents to the Communications Security Establishment within 72 hours

Read Bill C-8

US judge rules Anthropic's AI training is fair use

On 23 June 2025, a US judge ruled that AI start-up, Anthropic, did not infringe copyright by using books to train its large language model, Claude. The case was brought by three authors, including best-selling writer Andrea Bartz, who argued that Anthropic had used their copyrighted works without permission. The judge upheld Anthropic's 'fair use' defence, finding that the books were used to develop general language understanding, rather than to reproduce or distribute the content.

However, the court found that Anthropic did violate the authors' rights by downloading and storing over 7 million pirated books as part of its central library – an act not protected under fair use. A trial is scheduled for December to determine damages, which could reach up to $150,000 per infringed work.

Developers of AI models should carefully vet training data to avoid using pirated or unauthorised sources. Clear documentation, transparency of use, and legal oversight are key to managing copyright risks.

Read the ruling

Researchers uncover 'largest data breach in history'

A recent investigation by Cybernews has uncovered a staggering 16 billion compromised credentials, claiming it could be the largest leak in history. The data includes login details for social media, VPNs, developer portals, and user accounts from major vendors, such as Apple, Google, and various government services.

These credentials likely originated from infostealer malware on user devices, rather than a breach at the companies themselves. The leaked data spans 30 distinct datasets, many of which Cybernews believes to be entirely new (not recycled from older incidents).

The incident is a stark reminder that password-based security alone is no longer enough.

Organisations should:

- Require password resets, especially for employees accessing corporate systems and cloud services
- Adopt stronger access controls, such as multi-factor authentication (MFA), or move towards secure passkeys

- Promote the use of password managers and regular credentials monitoring
- Consider dark web monitoring and alerting tools to detect criminal activity

[For advice on creating strong passwords, storage methods, and effective management, read our blog](#).

UNITED KINGDOM

Deadline looms for online services under new child safety Codes

On 25 July 2025, the Protection of Children Codes will come into effect. Published by Ofcom in April under the Online Safety Act 2023 (OSA), the draft Codes outline how user-to-user and search services should meet their legal obligations to keep children safe online. They cover key areas, including age assurance, content moderation, governance, and user controls.

Organisations providing online services that are likely to be accessed by children must complete a children's risk assessment and adopt proportionate safety measures to mitigate identified harms before 24 July 2025.

The Codes aren't legally binding, but following them is the easiest way to demonstrate compliance with the OSA. Providers who deviate from the recommendations must justify how their alternative measures achieve the same level of protection.

[Read Ofcom's guidance](#)

EUROPEAN UNION

Committee approves new rules for cross-border GDPR enforcement

On 27 June 2025, the European Council's Permanent Representatives Committee approved the final text of the proposed GDPR Cross-Border Enforcement Regulation. It aims to streamline how authorities handle cross-border privacy cases and improve consistency, efficiency, and outcomes for individuals, whether cases arise from complaints or are initiated by regulators.

Key provisions include:

- Clear rules on complaint admissibility and handling
- Rights for individuals to communicate directly with their national authority
- Mandatory timelines for cooperation and dispute resolution between authorities
- Enhanced transparency and a guaranteed right for organisations under investigation to be heard

If adopted by the European Parliament at first reading, the Council will formally approve the regulation without further amendments. Some provisions will apply immediately, while others will take effect 15 months after the regulation enters into force.

Read the proposal

Italian DPA rules against use of private messages in workplace investigations

A recent ruling by the Italian Data Protection Authority (DPA) limits how employers can use third-party reports, private messages, or social media content in disciplinary proceedings.

The ruling follows a complaint from an employee who was dismissed after her employer used screenshots of private Facebook and WhatsApp conversations as evidence in a disciplinary hearing. The screenshots, which allegedly contained defamatory remarks about the employer, were submitted by colleagues and third parties and used to support two disciplinary actions.

The DPA concluded that:

- Using private messages, even if obtained passively, still counts as data processing under the GDPR
- The employer failed to justify that the messages were relevant or lawfully used
- Content shared in private chats or closed social media groups comes with a legitimate expectation of privacy
- Using such information in disciplinary action, without a clear legal basis, breached the GDPR principles of lawfulness, purpose limitation, and data minimisation
- A company's internal social media policy does not override an employee's data protection rights

As a result of its findings, the DPA ruled unlawful processing of personal data, and the company was fined €420,000.

Read the ruling

INTERNATIONAL

Vietnam passes Personal Data Protection Law

On 26 June 2025, the National Assembly of Vietnam passed the Personal Data Protection Law (PDPL). Scheduled to take effect on 1 January 2026, the PDPL aims to modernise data protection standards by introducing several new concepts not within the current Personal Data Protection Decree.

New provisions include:

- Clear definitions for personal and sensitive data
- Sector-specific provisions for fields like Healthcare, AI, and Finance
- Exemptions from Transfer Impact Assessments (TIAs) apply to employee data stored in the cloud and to individuals transferring their own data outside of Vietnam
- Five-year grace period for small enterprises and start-ups to allow for compliance
- Notable exemptions for micro-enterprises and household businesses

The new law also introduces significant penalties for violations, including fines of up to 10x the profit gained from data trading, 5% of annual revenue for cross-border breaches, and up to VND 3 billion (approximately $115,000 or £83,550) for other offences.

Learn more about the PDPL

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/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