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.

How social communication channels impact DSARs

The growing use of workplace social communication tools, such as Slack and Microsoft Teams, is bringing new challenges for companies that are already dealing with an increasing number of Data Subject Access Requests (DSARs).

In our latest blog, DPOs and DSAR specialists, Matt Spall and Pippa Scotcher, break down the complexities of handling DSARs in a world of constant messaging and casual conversations. From managing data on personal devices to navigating platform-specific export limitations, Matt and Pippa offer practical advice on how to ensure your organisation is DSAR-compliant.

How social communication channels impact DSARs

UNITED KINGDOM

UK DUA Bill could bring significant change to the Health sector

The UK Health and Care sector is poised for significant change with the introduction of the Data (Use and Access) Bill, which was presented to the House of Lords on 23 October 2024. The Bill aims to enhance data protection practices across a range of businesses and services in both the public and private sectors.

The proposed key updates include:

- Reforms to the Information Commissioner's Office (ICO)
- Changes to direct marketing and cookie enforcement
- Reintroduction of the recognised Legitimate Interests lawful basis
- Minor amendments to process requirements, such as data subject rights, international transfers, and automated decision-making

This legislation will also bring new information standards to Healthcare IT providers, which could result in significant compliance challenges for smaller organisations. In our latest article, Lawrence Carter, DPO and Life Sciences Sector Lead, shares insights on these changes and the potential impact for these businesses.

Read Lawrence's insights here

DSIT launches AI Management Essentials tool for SMEs

On 6 November 2024, the Department for Science, Innovation and Technology (DSIT) launched their draft AI Management Essentials (AIME) tool. The self-assessment tool is designed to support SME organisations in establishing management and risk assessment processes for developing responsible artificial intelligence.

At the same time, the DSIT launched a public consultation into the AIME tool to ensure it sufficiently helps organisations improve their AI governance processes. The consultation closes on 29 January 2025.

Find the AIME tool here

EUROPEAN UNION

CJEU allows GDPR claims in business litigation

In a landmark decision, the Court of Justice of the European Union (CJEU) has ruled businesses can sue competitors over GDPR violations under certain unfair competition laws. As a result, alleged GDPR infringements now expose organisations to potential competitive business litigation, as well as private litigation from affected data subjects and regulatory enforcement action.

As part of the ruling, the CJEU also expanded the definition of ‘health data’ to include information from online pharmacy orders, including names, delivery addresses, and product details. This could affect many organisations in the Life Sciences, Healthcare, and Consumer Goods sectors, who will face stricter GDPR protections relating to special category data.

Learn more about the ruling here

Irish DPC fines LinkedIn Ireland €310M for GDPR violations

The Irish Data Protection Commission (DPC) has fined LinkedIn Ireland €310M for violating the General Data Protection Regulation (GDPR). An inquiry into the social media giant found that LinkedIn did not have a valid legal basis for processing personal data for behavioural analysis and targeted advertising, as the consent obtained from users was not sufficiently informed or freely given.

The decision underscores the importance of adhering to the GDPR's principles, particularly Lawfulness, Fairness and Transparency. The Information Commissioner's Office (ICO) provides a comprehensive guide to understanding the seven principles of the GDPR, explaining how organisations can uphold them.

Read the ICO guidance here

NORTH AMERICA

OPC launches investigation into federal tax agency

On 29 October 2024, the Office of the Privacy Commissioner of Canada (OPC) launched an investigation into the Canada Revenue Agency (CRA) following cyberattacks that led to more than 30,000 privacy breaches over the last 4 years. The investigation will determine whether the CRA adhered to their obligations under Canada's Privacy Act, which include ensuring personal information is protected with appropriate security measures.

The OPC urges individuals to check their CRA accounts for suspicious activity and update their passwords.

Organisations can mitigate the consequences of data breaches by developing a long-term data breach management framework and security strategy. Our blog on **Data breach management** explores key best practices and provides organisations with 5 tips for an effective response.

White House publishes AI framework for military use

On 24 October 2024, the White House published the *Framework to Advance AI Governance and Risk Management in National Security*, designed to ensure the responsible use of artificial intelligence in military operations. The Framework outlines specific restrictions on AI use and mandates minimum risk management practices, such as impact assessments and appropriate human oversight.

In addition, the Framework requires covered agencies to:

- Conduct an annual inventory of their high-impact AI use cases
- Establish an AI Governance Board chaired by the Chief AI Officer
- Implement standardised training requirements on the use and development of AI

By requiring comprehensive oversight and risk assessments, the Framework will help safeguard sensitive data, reducing the risk of misuse or data breaches that could arise from poorly implemented AI technologies.

Read the Framework here

INTERNATIONAL

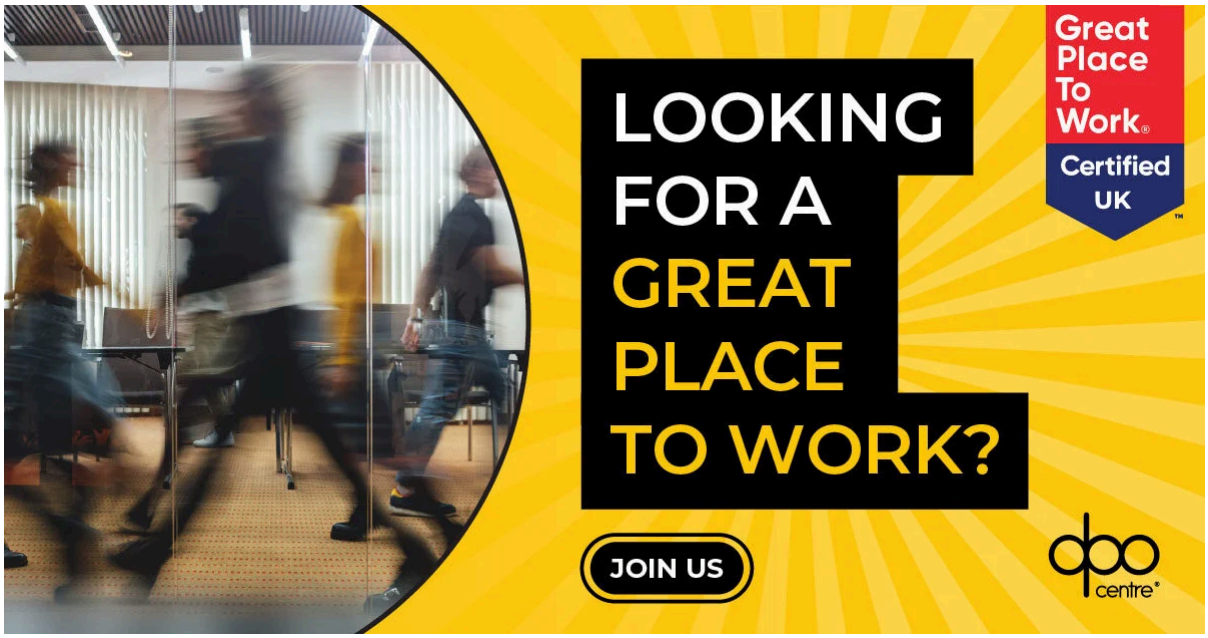
South Korea's PIPC fines Meta KRW 21.6B for privacy violations

On 5 November 2024, South Korea's Personal Information Protection Commission (PIPC) fined Meta Platforms Inc. KRW 21.6 billion (approximately €14.3M) for violating the Personal Information Protection Act. An investigation found the technology company had:

- Collected sensitive personal information, including religious and political views, of around 980,000 users without consent
- Shared sensitive data and behavioural information with advertisers for customised services
- Failed to implement protective measures to prevent data leaks through hacking

The PIPC also received complaints that Meta had denied users' rights to access their personal information without a justifiable reason.

This case underscores the critical role of data protection in **building customer trust** and ensuring compliance.



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)**

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