



WERELDWIJD PRIVACYNIEUWS
VAN DPO CENTRE

The DPA 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.

What is a DPA and why do you need one?

A Data Processing Agreement (DPA) is a necessary requirement between data controllers and data processors operating under the General Data Protection Regulation (GDPR). But aside from legal compliance, what is the benefit of having a DPA?

In our latest blog, we look at the main reasons why you need a DPA, some of the common misconceptions surrounding its use, and the key elements you should include in your documents.

[Read our latest blog](#)

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](#)

Dutch AP investigates holidays parks' use of FRT

The Dutch data protection authority, Autoriteit Persoonsgegevens (AP), recently investigated 8 holiday parks that use facial recognition technology (FRT) for entry into their leisure facilities. AP found that all 8 parks were in violation of the General Data Protection Regulation (GDPR), having failed to secure informed consent, offer an alternative entry mechanism, or inform guests sufficiently on how their data would be used.

Since the investigation, 7 parks have adjusted their way of working. However, AP has imposed an order on the remaining holiday park, which faces a fine or incremental penalty if they do not correct their FRT use before December.

Watch our webinar, **On face value: Understanding the privacy risks of Live Facial Recognition**, where FRT specialist Paul Collier examines the challenges of implementing this technology and shares innovative solutions for successful and compliant deployment.

[Watch the webinar on FRT and data protection](#)

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](#)

The graphic features a grid of puzzle pieces. The top-left piece contains the text 'Privacy Puzzle GLOBAL WEBINAR SERIES' and 'WATCH ALL 10 WEBINARS ON DEMAND'. Below this, it says 'Get insights from leading DPOs and industry insiders on some of the complex privacy challenges faced by organisations today.' and 'WATCH ON DEMAND'. The other puzzle pieces contain portraits of various individuals. The bottom right corner features the 'dpo centre' logo.

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](#)

A promotional poster for the IAPP Europe Data Protection Congress 2024. The poster has a yellow background with a blue rectangular area in the center. Inside the blue area, the text 'iapp' is in the top left, 'WE ARE EXHIBITING' is in large white letters, 'IAPP Europe Data Protection Congress 2024' is below it, followed by 'Training 18-19 November | Workshops 19 November' and 'Conference 20-21 November'. At the bottom of the blue area, 'BRUSSELS' is on the left and '#DPC24' is on the right. Below the blue area, there is a black bar with a calendar icon, '20-21 NOV 2024', 'BRUSSELS, BELGIUM', and the 'dpo centre' logo on the right.

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.

**ONS TEAM
GROEIT
WIL JE BIJ
ONS KOMEN
WERKEN?**



www.dpocentre.com/join-the-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 (The Netherlands)**
- **Data Protection Officer - Life Sciences (United Kingdom/The Netherlands)**
- **Data Protection Officers (United Kingdom)**
- **Data Privacy Officers (Canada)**
- **Data Protection Support Officers (United Kingdom)**
- **Copywriter (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](#)