WERELDWIJD PRIVACYNIEUWS
VAN DPO CENTRE

The DPIA 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.

Compliance with the AI Act Part 4: Essential Strategies

For organisations developing or deploying AI systems, keeping pace with AI regulations goes beyond compliance. It's a chance for businesses to spearhead responsible AI innovation and foster trust with users and regulators alike.

In the final chapter of our blog series, we explore **5 key strategies** that will help your business not only comply with the EU's AI Act but thrive in this rapidly evolving era of AI.

Read Part 4 here

EUROPEAN UNION

European AI Office publishes first draft of General-Purpose AI Code of Practice

On 14 November 2024, the European AI Office published the first draft of the General-Purpose AI Code of Practice. Written by independent experts, the Code will define the rules for providers of general-purpose AI models under the EU AI Act, focusing on transparency and copyright. It will also cover models that pose systemic risks, covering taxonomy, risk assessments, and mitigation measures.

Following publication of the first draft, stakeholders, EU Member State Representatives, and European and international observers now have until 28 November 2024 to provide feedback through working groups and written submissions.

Learn more in our news article, including insights from David Smith, DPO Centre DPO and AI Sector Lead.

Belgian DPA tightens rules on biometric data in workplaces

In a recent decision, the Litigation Chamber of the Belgian Data Protection Authority (DPA) ruled that employee consent for biometric data use, such as fingerprints, is typically invalid in workplace settings due to power imbalances. The case involved an employer using a fingerprint-based time tracking system, which an employee contested under GDPR

concerns. The DPA fined the employer €45,000 for failing to properly inform employees, relying on unclear and non-voluntary consent, and not conducting a mandatory Data Protection Impact Assessment (DPIA).

The DPA emphasised that employers should prioritise alternatives to biometric systems, such as time clocks or access cards, wherever feasible. When biometric data is used, it must also be supported by clear purposes, ensure the data processing is kept to a minimum, and strictly adhere to GDPR safeguards to avoid sanctions.

For further information, read our blog: **The do's and don'ts of processing biometric data**

Dutch DPA finds DUO algorithm discriminatory, violating the GDPR

The Dutch data protection authority, Autoriteit Persoongegevens (AP), has found that an algorithm used by the Education Executive Agency (DUO) is discriminatory and, therefore, violates the GDPR and other EU laws. The algorithm was designed to assess risk factors for potential abuse of grants by non-resident students. However, an AP investigation found that the criteria used, which included education type, distance, and age, lacked objective justification.

When using an algorithm with selection criteria, organisations should justify the selection criteria objectively and test the algorithm outcomes in advance.

Read more about the case here

UNITED KINGDOM

ICO publishes priorities for protecting children's personal information online

The Information Commissioner's Office (ICO) has announced its 2024-2025 priorities for protecting children's personal information online. The ICO will focus on social media and video-sharing platforms, paying particular attention to:

- Enforcing default privacy and geolocation settings
- Restricting profiling children for targeted advertisements
- Regulating the use of children's data in recommender systems
- Monitoring consent for processing the data of children under 13 years

In line with the Children's Code of Practice, launched in 2021, organisations should ensure that children's profiles are set to private, geolocation is disabled, and profiling is turned off by default, as well as using secure parental consent mechanisms.

Find further information on the Children's code here

NORTH AMERICA

32 State Attorneys General urge Congress to pass Kids Online Safety Act (KOSA)

On 18 November 2024, a coalition of 32 Attorneys General called on Congress to pass the bipartisan Kids Online Safety Act (KOSA) before the end of the year. Led by Tennessee Attorney General, Jonathan Skrmetti, the letter emphasised the growing crisis of youth mental health due to social media use.

If passed, KOSA would strengthen online protections for minors through several key provisions, including:

- Requiring platforms to automatically enable their strongest safety protections for minors
- Allowing young users and parents to disable manipulative design features and algorithmic recommendations
- Providing parents with new tools to identify harmful behaviours

- Improved capabilities to report dangerous content

Read the letter here

OPC adopts resolution to combat deceptive design patterns

The Office of the Privacy Commissioner of Canada (OPC) and privacy regulators across Canada have adopted a joint resolution to address privacy-related harms resulting from deceptive design patterns. The resolution calls for public and private sector organisations to avoid platform designs that could influence or manipulate users into making decisions that go against their privacy interests.

The OPC highlighted their expectations for organisation websites and apps:

- Incorporate Privacy by Design
- Limit personal data collection to that which is necessary for the intended purpose
- Promote transparency when collecting personal information
- Examine and test the design architecture and usability
- Choose design elements that adhere to privacy principles found in Canadian law

Read the resolution here

INTERNATIONAL

Cameroon introduces Personal Data Protection Bill to Parliament

The government of Cameroon has introduced the Personal Data Protection Bill to Parliament, which aims to modernise the country's approach to data protection. The Bill will govern how personal data is collected, stored, and processed, aligning Cameroon with global efforts to address the risks of data misuse.

The Bill will also establish a Personal Data Protection Authority, responsible for issuing authorisations, approving certification mechanisms, handling complaints, and coordinating with other governmental agencies.

Learn more about the Bill here

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