



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.

## How data protection builds customer trust and loyalty

Since the General Data Protection Regulation (GDPR) was implemented in 2018, public awareness of privacy rights has continued to grow. Organisations must recognise that safeguarding personal data is a key factor in building customer trust and loyalty.

In our latest blog, we explore how transparent communication about data handling and adopting Privacy by Design practices are not only vital for meeting data protection regulations but also for fostering strong customer relationships.

[Read our blog here](#)

## UNITED KINGDOM

### Data (Use and Access) Bill introduced in House of Lords

On 23 October 2024, Baroness Jones of Whitchurch introduced the Data (Use and Access) Bill, which aims to update the UK's current data protection and privacy laws. The Bill reflects the commitments made on 17 July 2024 in the King's Speech, where the new Labour government outlined plans to modernise and strengthen data protection and privacy legislation with an upcoming, now presumed defunct, Digital Information and Smart Data (DISD) Bill.

Passing its first reading in the House of Lords, the proposed DUA Bill will now face further scrutiny and debate. Privacy professionals and stakeholders across various sectors will be watching closely as the Bill progresses.

Learn more about the proposed Bill and read our DPO's initial insights in our latest news story.

[Read our DUA Bill news story.](#)

### NCSC updates MFA guidance

On 9 October 2024, the National Cyber Security Centre (NCSC) announced updates to its Multi-Factor Authentication (MFA) guidance to tackle the rising threats from cyber attackers intercepting MFA keys. The guidance explores the strengths and weaknesses of

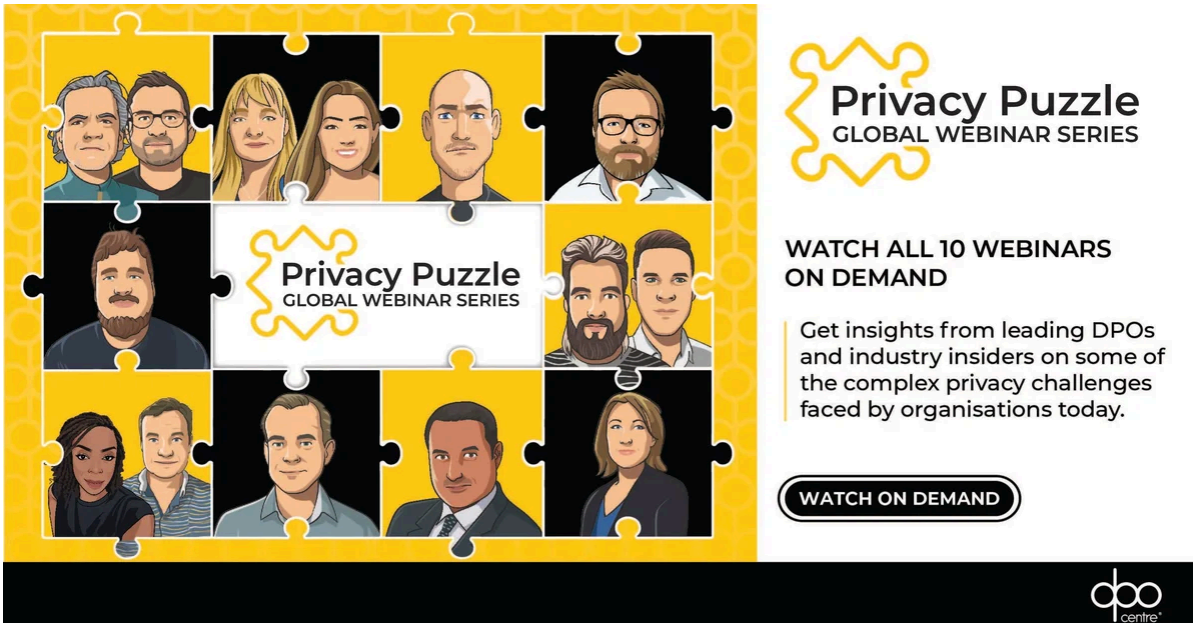
MFA implementations, helping organisations choose the strongest and most practical type of MFA for their needs.

MFA is a crucial step in protecting data and is a regulatory requirement for many industries, such as Healthcare and Finance. By implementing a second layer of verification, organisations make it significantly harder for cybercriminals to gain unauthorised access.

The NCSC recommends organisations:

- Use a service that uses phishing-resistant MFA by default
- Mandate strong MFA for every user accessing sensitive data
- Use trusted devices to make strong MFA achievable and easier
- Avoid MFA anti-patterns, such as time-based re-authentication

[Read the NCSC guidance here](#)



The graphic features a grid of puzzle pieces with cartoon avatars of various people. A central white puzzle piece contains the text "Privacy Puzzle GLOBAL WEBINAR SERIES". To the right, the text "Privacy Puzzle GLOBAL WEBINAR SERIES" is displayed above a yellow puzzle piece icon. Below this, it says "WATCH ALL 10 WEBINARS ON DEMAND" and "Get insights from leading DPOs and industry insiders on some of the complex privacy challenges faced by organisations today." A "WATCH ON DEMAND" button is at the bottom right. The dco centre logo is in the bottom right corner.

## EUROPEAN UNION

### Deadline passes for NIS2 Directive transposition

By 17 October 2024, all EU Member States were required to adopt and publish the necessary measures to implement the Network and Information Systems Directive 2 (NIS2). The Directive aims to enhance the resilience and security of critical infrastructure within the European Union by establishing stricter security requirements and expanding its scope to more sectors.

Under NIS2, in-scope organisations must enhance their cybersecurity measures and establish incident reporting procedures. Businesses should familiarise themselves with how NIS2 has been implemented in jurisdictions in which they are regulated.

[Find helpful guides on NIS2 here](#)

### Dutch government publishes guide for EU AI Act

On 16 October 2024, the Dutch government published a guide for the European Union's Artificial Intelligence Act (EU AI Act). It ensures organisations in the Netherlands can systematically address each aspect of the Act and prepare for its implementation by providing a detailed explanation of the different risk categories for AI systems, alongside compliance measures. The guide also provides advice on transparency and accountability, standards for data management, and details on certification processes.

[Read the Dutch guide here](#)

For organisations outside the Netherlands, you can find a comprehensive breakdown of the EU AI Act in our 4-part blog series, [Compliance with the AI Act](#). The series explores key deadlines for implementation, the risk-based approach to the classification of AI systems, in-scope organisations and their requirements, and essential strategies for compliance.



**WHO CAN APPLY TO OUR CHARITY & COMMUNITY FUND?**

Eligible organisations must

- ✓ Be based in the UK
- ✓ Have a management committee of at least 3 unrelated people
- ✓ Have a bank account in the name of the charity/NFP

**FIND OUT MORE**

**dpo**  
centre®

## NORTH AMERICA

### New financial rule includes consumer privacy protections

On 22 October 2024, America's Consumer Financial Protection Bureau (CFPB) finalised the Personal Financial Data Rights Rule, bringing significant privacy protections to individuals' data. Under the new Rule, personal financial data can only be used for the purposes requested by the consumer, and third parties cannot collect, use, or retain consumers' data for their own unrelated business purposes. Furthermore, when a consumer revokes access, firms must end data access immediately and delete the data by default.

The compliance deadline for financial firms will vary by size. Large organisations must comply by 1 April 2026, whilst the smallest in-scope organisations have until 1 April 2030.

[Learn more about the Rule here](#)

## Internet Archive experiences third breach in one month

The Internet Archive, a nonprofit digital library, has confirmed a third security breach in one month. At the end of September, the site experienced a major cyberattack that compromised the personal data of approximately 31 million users, including email addresses, usernames, and Bcrypt-hashed passwords.

Following the breach, the Internet Archive failed to adequately secure their system, leading to two further breaches on 9 and 20 October. In both cases, hackers accessed the archive's Zendesk platform using unrotated API tokens – digital keys used to authorise access to systems. The breach exposed user data, including personal identification documents, stored in support tickets dating back to 2018.

These attacks underscore the importance of effective data breach management.

Read our [Data breach management blog](#) for 5 essential strategies for an effective response.

---

## INTERNATIONAL

## Australia's OAIC publishes privacy guidance for AI models

The Office of the Australian Information Commissioner (OAIC) has published guidelines on privacy considerations for organisations deploying artificial intelligence (AI) models. The guidance is designed to help organisations comply with their privacy obligations when using commercially available AI products.


Key measures for organisations:

- Ensure that any personal information input into an AI system, as well as the output data generated, complies with privacy laws
- Conduct due diligence to ensure the product is suitable for its intended uses
- Establish policies and procedures for the use of AI systems, providing clear and transparent information about their use of AI
- Comply with the Australian Privacy Principles (APPs) if AI systems generate or infer personal information
- Ensure secondary use of personal information is within reasonable expectations of the individuals or gain explicit consent
- Avoid entering personal information into publicly available generative AI tools

[Read the guidance here](#)

---





**LOOKING FOR A GREAT PLACE TO WORK?**

**JOIN US**

Great Place To Work®  
Certified UK

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 (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](#)