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.

Bring Your Own Device (BYOD) risk management guide

Bring Your Own Device (BYOD) policies support flexible working, but they also reduce organisational control over how business systems and data are accessed. As employees increasingly use personal devices for work, traditional safeguards such as MFA and VPNs may not address the full range of risks.

Our latest blog explores the hidden risks of unmanaged personal devices and regulator expectations around risk-based approaches. We provide practical steps organisations can take to strengthen BYOD controls and protect sensitive data.

Read our blog

UNITED KINGDOM

ICO publishes report on automation in recruitment

The report is based on discussions between the Information Commissioner's Office (ICO) and employers, highlighting the need for stronger safeguards and greater transparency when using automated decision-making (ADM) in recruitment.

The report calls on organisations to review how automated tools are used in hiring processes, particularly where decisions may significantly affect job applicants.

The ICO also sets out expectations for organisations, including:

- Proactively monitor for bias and mitigate associated risks
- Be transparent with candidates about the use of ADM and how it works
- Clearly explain individuals' rights, including how to challenge decisions

Read the report

FCA and ICO issue joint statement on handling vulnerability-related data

The Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO) have issued a joint statement clarifying regulatory expectations for firms processing vulnerability-related data.

The statement aims to support organisations in balancing data protection requirements with the need to identify and assist customers in vulnerable circumstances, particularly under the FCA's Consumer Duty.

It highlights the importance of sharing relevant information appropriately across the distribution chain, monitoring outcomes for vulnerable consumers, and ensuring data is used in a way that is fair, transparent, and proportionate.

Read the joint statement

EUROPEAN UNION

EDPB and EDPS issue joint opinion on EU cybersecurity proposals

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have adopted a joint opinion on the European Commission's proposals for a Cybersecurity Act 2 and targeted amendments to the NIS2 Directive.

The proposals aim to strengthen cybersecurity across the EU whilst simplifying compliance for organisations. The joint opinion broadly supports these objectives, including enhancing the role of the European Union Agency for Cybersecurity (ENISA) and promoting greater uptake of cybersecurity certification schemes.

However, the EDPB and EDPS emphasise that cybersecurity measures must align with data protection principles, ensuring processing remains necessary and proportionate whilst avoiding fragmented or duplicative compliance obligations.

Read the opinion

CNIL publishes framework on HR data retention periods

Published on 2 April 2026 by the French data protection authority (CNIL), the framework provides practical guidance on how long different categories of employee and candidate data may be retained.

The guidance aims to support compliance with the GDPR storage limitation principle. It emphasises that retention periods must be proportionate and justified, considering legal obligations as well as operational needs.

The CNIL highlights the need to:

- Define clear, purpose-based retention periods
- Distinguish between active data and archived records
- Ensure personal data is deleted or anonymised once no longer required
- Document retention rules and inform individuals how long their data will be kept

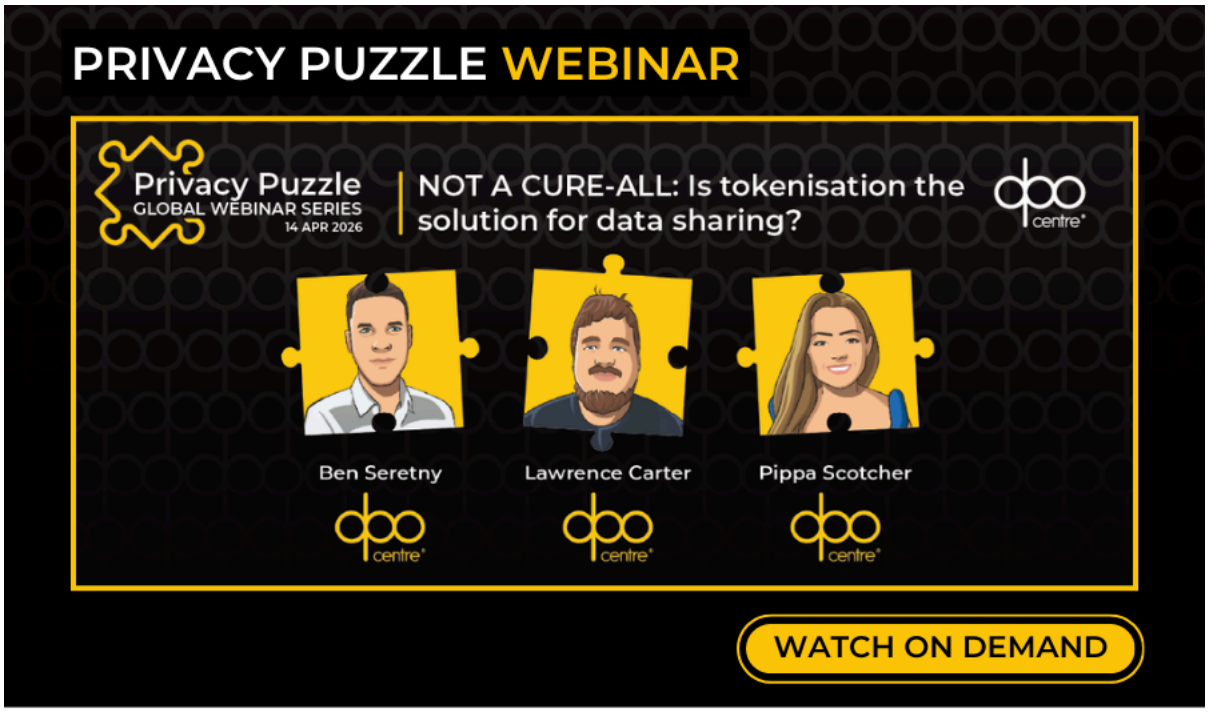
Download the framework

Dutch National Police experience breach following phishing attack

The force's Security Operations Centre detected the incident quickly and blocked unauthorised access. Authorities confirmed that citizens' data was not affected, but it is currently unclear whether any employee data was compromised.

The incident highlights the continued effectiveness of phishing attacks, even in highly secure environments. Organisations should ensure robust safeguards are in place, including employee awareness training, multi-factor authentications, and continuous monitoring to detect and respond to suspicious activity quickly.

Read our blog to learn more about safeguarding your organisation against phishing attacks.



CANADA & UNITED STATES

Iowa Attorney General sues Change Healthcare over data breach

The breach occurred in 2024 and affected nearly 2.2 million residents. It exposed highly sensitive personal data, including Social Security numbers, health insurance details, and medical records.

The lawsuit alleges that outdated IT infrastructure, inadequate incident response, and significant delays in notifying affected individuals contributed to the scale and impact of the incident.

The case highlights the importance of timely breach detection, effective incident response, and prompt notification to individuals. Organisations should ensure robust response plans are in place and regularly tested to minimise impact and meet regulatory expectations.

Read our blog on managing data breaches effectively.

Global sweep highlights gaps in children's online privacy protections

The Privacy Commissioner of Canada, alongside 26 data protection authorities, has concluded a Global Privacy Enforcement Network (GPEN) sweep examining how websites and mobile applications handle children's personal data.

The review assessed nearly 900 services, focusing on transparency, age assurance mechanisms, and the use of privacy controls to limit data collection. Whilst good practices were observed overall, concerns were raised around increased data collection requirements, greater sharing of personal data with third parties, and age checks that can be easily bypassed.

The findings highlight the need for stronger safeguards when designing services likely to be accessed by children, particularly around data minimisation and effective age assurance.

Read the GPEN sweep report

INTERNATIONAL

Japan approves amendments to data protection law

On 7 April 2026, the Cabinet of Japan approved proposed amendments to the Act on the Protection of Personal Information (APPI), introducing a range of updates to strengthen data protection and address emerging technologies.

The proposed changes include expanded consent exemptions for certain AI-related processing, enhanced protections for minors, and new obligations governing the use of facial recognition data. The amendments also introduce strengthened enforcement powers for regulators.

Organisations operating in Japan should review their data processing activities to assess how the proposed changes may impact compliance requirements.

Learn more

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 Officers - Life Sciences (United Kingdom)**
- **Data Protection Coordinator - Life Sciences (Poland)**
- **Financial Controller (United Kingdom)**
- **Senior Commercial Executive (United Kingdom)**
- **Senior HR Advisor - maternity cover (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, **recognised as one of the UK's Best Workplaces™ for medium-sized businesses**, [apply today!]

FOLLOW US ON LinkedIn