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.

Privacy Management Platforms: A practical guide for strengthening privacy operations

Privacy Management Platforms (PMPs) can ease DPO workloads, improve cross-functional collaboration, and give privacy programmes the structure they need to grow. But finding the right platform means looking beyond its key features to ensure it fits your organisation's processes, scales with your needs, and keeps DPOs at the centre.

In our latest blog, experts from Dastra, Wired Relations, and TrustWorks share insights on the benefits of PMPs, why DPO input remains critical, and how to choose and implement a platform that boosts compliance, accountability, and resilience.

Read our blog

UNITED KINGDOM

UK's Law Commission highlights personal data risks in AI development

On 31 July 2025, the Law Commission of England and Wales published a discussion paper on the legal implications of artificial intelligence. It highlights the challenges AI creates for compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, especially when personal data is involved.

Modern AI is trained on vast datasets, which often include people's personal data. This raises well-known concerns about whether AI systems can meet core data protection obligations, such as:

- Being transparent about how personal data will be processed
- Ensuring processing is lawful, fair, and as individuals would reasonably expect
- Relying on lawful bases, such as Consent or Legitimate Interests
- Demonstrating necessity and proportionality when using Legitimate Interests

The paper also notes that the complexity of AI systems can make it difficult for organisations to clearly explain how personal data will be used, making it harder to obtain valid consent.

The paper calls for further consideration of how data protection obligations can be met in the context of opaque and adaptive AI models. It advises organisations to review their AI systems regularly to ensure lawful bases remain valid and privacy information stays accurate.

Read the discussion paper

NCSC updates Cyber Assessment Framework to address evolving threats

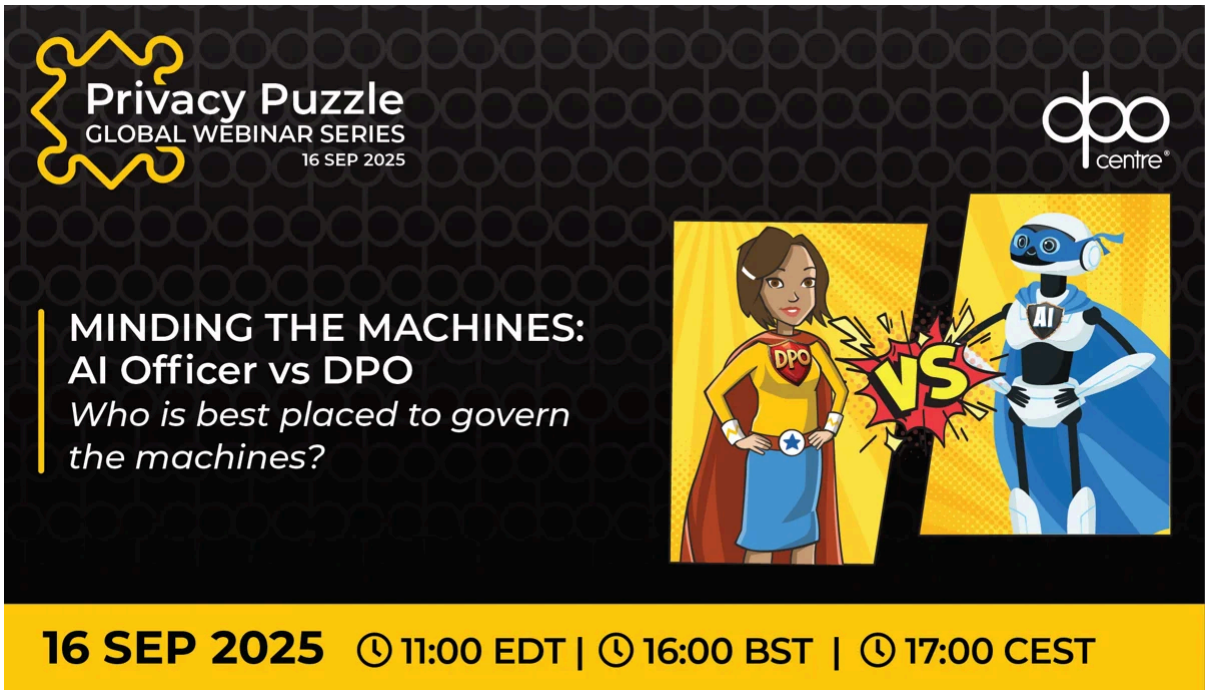
On 6 August 2025, the UK's National Cyber Security Centre (NCSC) updated its Cyber Assessment Framework (CAF) in response to the growing cyber threat to critical services. The CAF helps organisations strengthen cyber resilience and meet legal and regulatory requirements.

The updates aim to help providers of essential services close the widening gap between escalating threats and their ability to defend against them, while also strengthening the protection of personal data handled in the delivery of those services.

Key changes in CAF version 4.0 include:

- A new section on understanding attacker methods and motivations to inform cyber risk decisions
- Guidance on ensuring software used in essential services is developed and maintained securely
- Updates to security monitoring and threat hunting to improve threat detection
- Improved coverage of AI-related cyber risks throughout the framework

Read the Cyber Assessment Framework



EUROPEAN UNION

Irish DPC publishes toolkit to safeguard vulnerable adults' data

The Irish Data Protection Commission (DPC) has launched an Adult Safeguarding Toolkit to support organisations and individuals in protecting the personal data of vulnerable adults. The resource is designed to help ensure compliance with data protection law while promoting best practice in handling sensitive information.

The toolkit provides detailed guidance on collecting, using, storing, and sharing data about vulnerable adults in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. It includes practical advice, templates, and real-world examples to help embed effective data protection measures.

Topics covered include the core principles of data processing, data subject rights, and considerations for lawful and proportionate data sharing in safeguarding contexts. The DPC developed the resource in collaboration with healthcare, advocacy, and regulatory stakeholders to ensure it reflects the needs of those working directly with at-risk individuals.

Download the Toolkit

Italy aligns Cybersecurity Perimeter rules with NIS2 and GDPR requirements

On 1 August 2025, Italy's Council of Ministers approved a regulation updating the National Cybersecurity Perimeter. Set to take effect on 16 August 2025, the regulation applies to both public and private entities responsible for essential State functions or services critical to national interests.

In-scope organisations must promptly report cybersecurity incidents to the Italian National Cybersecurity Agency (ACN), implement robust security and risk-management measures,

and comply with requirements for incident response, service continuity, and data protection.

Data protection implications include:

- Strengthening safeguards around personal data through tighter incident reporting and risk-management protocols
- Ensuring continuity and resilience in service delivery, reducing the likelihood of breaches or data-loss incidents
- Reinforcing accountability and transparency around ICT procurement decisions involving systems that handle personal or critical information

The updated Perimeter complements the NIS2 Directive's focus on resilience and incident reporting while supporting the GDPR's requirements to protect personal data and respond effectively to breaches. In-scope entities should start preparing now to ensure their cybersecurity and data protection measures meet the new standards.

Read the Regulation

Hackers steal cervical cancer screening data of 485K women

Personal health data from nearly 485,000 women who participated in a national cervical cancer screening programme has been stolen in a cyberattack.

The breach occurred at Clinical Diagnostics NMDL, a third-party laboratory used by Population Screening Netherlands to analyse test results. The Nova cybercrime group reportedly stole 300GB of data in July, including names, addresses, dates of birth, social security numbers, and medical results. On 12 August 2025, Nova published part of the stolen data on the dark web.

Dutch authorities have raised concerns about the potential consequences for those affected, including fraud, reputational harm, and loss of trust in screening programmes.

The incident highlights the importance of robust vendor due diligence, particularly when third parties process large volumes of sensitive health data. **Read our blog** for 5 practical steps on assessing and managing vendor risk.

CANADA & UNITED STATES

OpenAI removes ChatGPT sharing tool amid privacy concerns

On 1 August 2025, OpenAI removed ChatGPT's public chat-sharing feature following concerns that sensitive conversations were being indexed by Google and other search engines. The experimental tool was designed to showcase informative chatbot interactions by allowing users to make specific chats publicly searchable by opting in through a 'Make this chat discoverable' setting.

Shared content was anonymised and required multiple opt-in steps, but reports surfaced of indexed chats containing sensitive topics, such as mental health and workplace issues. OpenAI believed the instructions made the implications clear but acknowledged that some users may have unintentionally exposed personal information. The company has since confirmed it is working with search engines to delist any content that was indexed.

The feature's removal underscores the privacy risks of publishing AI conversations in a searchable format. Organisations offering public-sharing tools should ensure robust safeguards, clear user communication, and regular reviews of privacy settings to prevent accidental exposure of personal information.

Find out more

Workday's AI hiring tool faces scrutiny over automated decision-making

A federal judge in California has ruled that software vendor Workday must provide an exhaustive list of employers who enabled its HiredScore AI features in their hiring processes.

The case stems from a collective action lawsuit that alleges Workday's AI-driven applicant recommendation system — which uses automated decision-making and profiling to score, sort, and rank applicants — disadvantaged candidates over age 40. The judge has expanded the collective's scope to cover all applicants processed using the HiredScore AI features.

Workday acquired HiredScore after the original complaint was filed and argued that the platform was a separate product and should therefore be excluded. The court rejected this, emphasising the functional integration into Workday's hiring platform, and ordered the company to submit the customer list by 20 August 2025.

The ruling comes amid growing scrutiny of algorithmic hiring tools and their potential to introduce bias. For a deeper look at the opportunities and risks of AI in recruitment, watch our webinar **SMART HIRING OR BACKFIRING: Employing AI in recruitment**.

INTERNATIONAL

Vietnam enacts landmark Law on Personal Data Protection

Vietnam has passed the Law on Personal Data Protection (PDP Law), strengthening and expanding the provisions of Decree 13. Effective from 1 January 2026, it applies to organisations operating in or engaging with Vietnam, including those processing the personal data of Vietnamese citizens without a physical presence in the country.

The PDP Law retains Decree 13's requirement for certain organisations, such as those processing sensitive data or making cross-border transfers, to appoint a Data Protection Officer (DPO) and conduct Transfer Impact Assessments (TIAs). A five-year grace period applies for startups and small businesses to meet these obligations, with limited exemptions.

Other changes include stricter consent rules, six defined data rights, new exemptions to TIA obligations, and sector-specific requirements.

Penalties are substantial, with fines of up to 10 times the revenue from trading personal data or 5% of annual revenue for cross-border transfer violations, alongside possible criminal sanctions.

Learn more about the PDP Law

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 Officers (The Netherlands)**
- **Data Protection Officers (EU)**
- **Data Protection Officers - Life Sciences (United Kingdom/Europe/Canada)**
- **Data Protection Support Officers (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, **ranked in the top 50 of the UK's Best Workplaces™ for medium-sized businesses**, **apply today!**

FOLLOW US ON LinkedIn