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.

CRM data retention: Balancing commercial objectives with GDPR compliance

Customer Relationship Management (CRM) systems are essential for driving growth, but without effective retention policies, they can quickly become a compliance liability.

In our latest blog, we explore how to build a data retention policy that balances business needs with GDPR obligations. Featuring expert insights from HubSpot, filerskeepers, and The DPO Centre, we break down what a 'healthy' CRM looks like – and how to get there.

Read our blog

UNITED KINGDOM

UK to regulate police use of facial recognition technology

The UK Home Office has confirmed plans to introduce a legal governance framework for law enforcement's use of facial recognition technology. The government is working closely with police forces to develop clear standards for deployment, aiming to address growing concerns over unchecked expansion of the technology.

The move follows repeated calls from Parliament and civil society for statutory regulation, amid fears that facial recognition is being adopted by police without adequate scrutiny, transparency, or oversight. Critics have warned that the current patchwork of guidance and case law is insufficient to protect individual rights.

By establishing a clear legal basis and oversight structure, the Home Office hopes to provide both accountability and assurance, helping police forces adopt facial recognition responsibly while maintaining public trust.

Watch our on-demand webinar on Live Facial Recognition to gain innovative solutions for successful deployment of LFR technologies.

ICO publishes guidance on profiling tools for online safety systems

On 30 July 2025, the Information Commissioner's Office (ICO) published new guidance clarifying how organisations can deploy profiling tools in trust and safety systems while complying with UK data protection law.

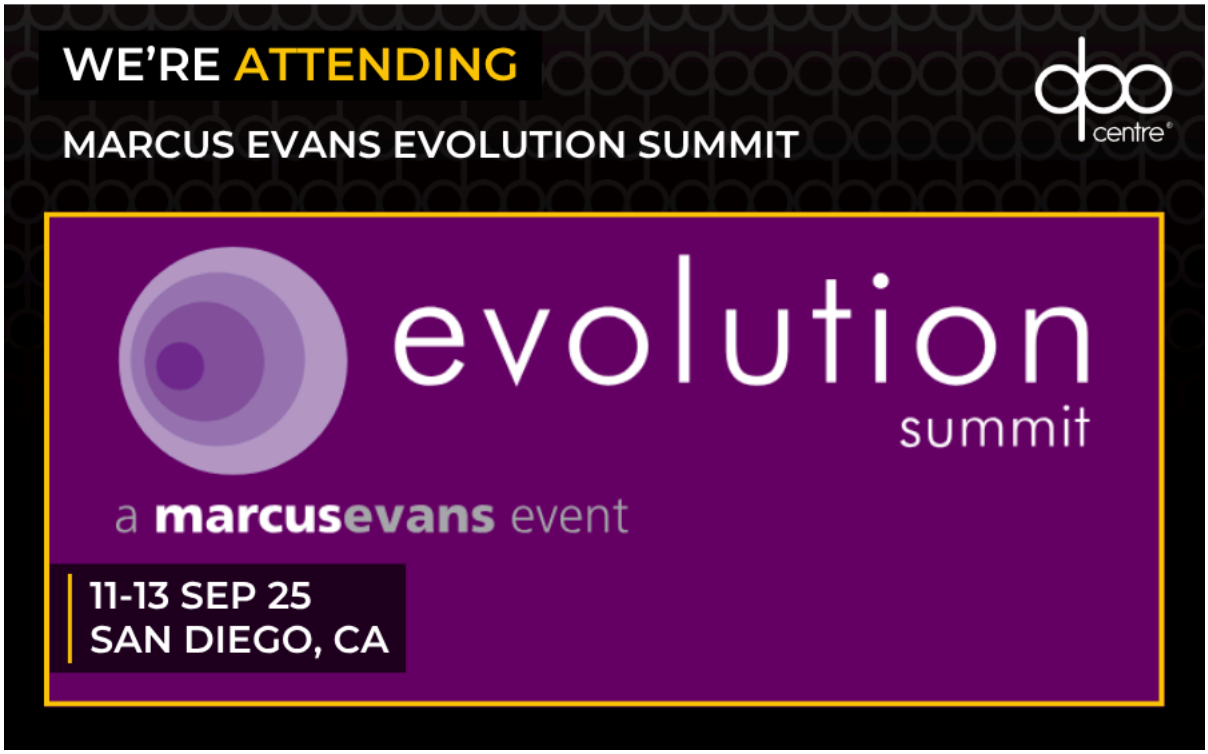
The ICO defines profiling tools as those that *'analyse aspects of a person's characteristics, behaviour, interests, or preferences'* to identify and mitigate online harms. The guidance outlines how organisations can ensure compliance with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and, where applicable, the Privacy and Electronic Communications Regulations (PECR).

Key sections cover:

- How profiling fits within trust and safety systems
- Relevant lawful bases and the application of data minimisation and purpose limitation principles
- When PECR rules apply to profiling conducted through cookies or similar technologies
- Steps organisations can take to demonstrate compliance, such as risk assessments and clear documentation

The guidance provides much-needed clarity for organisations navigating the overlap between online safety obligations and data protection responsibilities.

Read the ICO guidance



EUROPEAN UNION

CNIL opens consultation on web filtering gateway recommendation

On 28 July 2025, the French Data Protection Authority (CNIL) launched a public consultation on a draft recommendation regarding the use of web filtering gateways. These tools are commonly used by organisations to monitor or block employee access to certain online content, often for cybersecurity or productivity purposes.

The recommendation aims to provide legal certainty to data controllers using these solutions while encouraging service providers to adopt a Privacy by Design approach in line with GDPR principles. It applies to organisations deploying network-level filtering systems that manage web access for employees, service providers, or external visitors using their networks.

View the draft recommendation and take part in the consultation, which is open until 30 September 2025.

European Commission unveils transparency template for GPAI

On 24 July 2025, the European Commission published a standardised template to help general-purpose AI (GPAI) providers comply with transparency obligations under the EU AI Act. From 2 August 2025, newly placed GPAI models must include a summary of the training data used, while existing models have until 2027 to meet the same requirement.

Designed to support consistent and structured disclosures, the template balances transparency with commercial confidentiality. Key fields include:

- Provider and model identification
- Types and volume of training data

- Data sources
- Measures to exclude unlawful or biased data
- Steps to safeguard copyright and trade secrets

Non-compliance may result in penalties up to €15 million or 3% of global turnover. Providers are encouraged to adopt the template early to prepare for forthcoming regulatory expectations.

Download the template

Dutch DPA labels AI emotion recognition ‘dubious and risky’

On 15 July 2025, the Dutch data protection authority, Autoriteit Persoonsgegevens (AP), published its fifth *Report on AI & Algorithms in the Netherlands (RAN)*. The report focuses on the use of emotion recognition with AI and warns that the practice is ‘dubious and risky’.

It is particularly critical of emotion recognition technology deployed in customer services, wearable devices, and language models. The AP emphasised that mapping biometric characteristics, such as facial expressions or voice, to emotional states is inherently unreliable given cultural and individual variation. The AP noted that the potential for misinterpretation is high, especially when these systems influence decisions affecting individuals’ privacy or autonomy.

The EU AI Act already prohibits emotion recognition systems in schools and workplaces. Companies deploying such systems must rigorously assess legal and ethical viability under the General Data Protection Regulation (GDPR) and the AI Act. The AP suggests that where emotion detection offers only speculative benefit, organisations should opt for safer alternatives.

Read the report

CANADA & UNITED STATES

The White House publishes controversial AI Action Plan

On 23 July 2025, the Trump administration unveiled **Winning the Race: America's AI Action Plan**, a national strategy aimed at securing US dominance in artificial intelligence.

The plan outlines over 90 federal actions across three pillars:

1. Accelerating innovation
2. Building American AI infrastructure
3. Leading in international diplomacy and security

The plan focuses on deregulation, open-source development, and AI exports, while limiting funding for states with stricter AI laws — representing a clear shift from the previous focus on civil rights, transparency, and algorithmic risk mitigation.

Read our latest article for early perspectives from our AI Sector Lead on the new US strategy, with practical takeaways for organisations navigating transatlantic AI regulation.

Clorox files $380M lawsuit against IT vendor following major breach

On 23 July 2025, Clorox filed a lawsuit against its IT service provider, Cognizant, alleging that weak identity checks led to a major cyberattack in 2023. The breach allegedly began when a hacker impersonated Clorox employees over the phone and was granted password and MFA resets without proper checks.

Clorox says Cognizant repeatedly assured them that support agents were following agreed protocols, but the cybercriminal was able to access the network and escalate privileges across multiple accounts. This resulted in weeks of disruption and losses totalling $380 million.

The case highlights the need for strong internal governance, vendor oversight, and staff training. Organisations must ensure that third-party helpdesks enforce robust identity checks and log all access requests, particularly those involving credentials or MFA.

For practical steps on assessing vendor risks, read our blog on **GDPR-compliant vendor due diligence**.

INTERNATIONAL

China launches new DPO registration portal

The Cyberspace Administration of China (CAC) has launched a new online portal for registering Data Protection Officers (DPOs), marking a significant administrative change under China's Personal Information Protection Law (PIPL).

Registering a DPO has long been mandatory, but the portal now provides a formal mechanism for organisations that process the personal data of 1 million or more

individuals to submit required details to the regulator.

Organisations must provide the DPO's contact information, as well as details about their processing activities. This includes (but is not limited to) the categories of personal data handled, the number of monthly data subjects, and any cross-border transfers. Importantly, overseas organisations are also in scope if they process personal data of individuals in China.

Data controllers that already meet the requirements have until the 29 August 2025 to register their DPO, while organisations meeting the 1M threshold after the 18 July have 30 working days to submit their reports.

Register your DPO

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