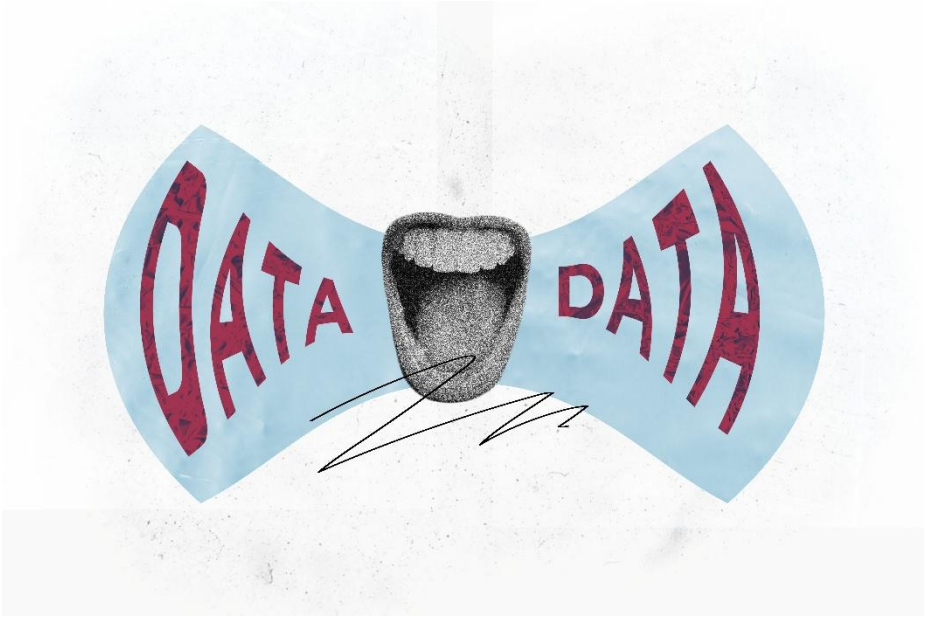
Privacy Partnership
AUGUST NEWSLETTER



UK BEGINS DATA (USE AND ACCESS) ACT ROLLOUT WITH COMMENCEMENT

The UK has started implementing the Data (Use and Access) Act 2025 **(DUAA)**, marking the start of a shift in the country's data protection law framework.

Some initial provisions came into force on 19 June 2025 - the day on which DUAA received Royal Assent and initiated its phased rollout.

On 20 August 2025, the government initiated a second wave of provisions through the first Commencement Regulations - which were made on 21 July 2025.

Notable provisions include:

The power of the Secretary of State to add new special categories of data to the UK GDPR

The requirement for the regulator to encourage expert public bodies to develop codes of conduct on using personal data for law enforcement.

The establishment for a court procedure relating to data subject access requests.

The DUAA introduces a wide range of targeted reforms across the UK GDPR, Data Protection Act 2018, and Privacy and Electronic Communications Regulations (**PECR**).

INSIDE THIS ISSUE

PRIVACY PARTNERSHIP

These changes impact several areas including legitimate interests' grounds, scientific research, automated decision-making and open banking. The government plans to implement most of the remaining provisions gradually over the next two to twelve months, with further commencement dates to follow through secondary legislation.

Meanwhile, the European Commission has taken steps to preserve data flows between the UK and the EU. On 22 July 2025, it launched the process to adopt new adequacy decisions - ensuring personal data can continue to move freely between the UK and the European Economic Area. This followed a six-month extension in June of the UK's existing adequacy status, which gave the Commission time to assess the implications of the DUAA.

Having reviewed the new UK framework, the Commission concluded that the UK continues to provide data protection safeguards that are essentially equivalent to those in the EU.

Michael McGrath (Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection) stated as follows regarding the significance of this development:

"The unobstructed flow of personal data between the EU and the UK is essential for many businesses, public authorities and individuals on both sides of the Channel. With this step, we are ensuring that this vital link stays open - not only to support commerce and research, but also to enable effective cooperation in criminal justice and law enforcement."

The Commission will now send the draft adequacy decisions to the European Data Protection Board for its opinion, seek approval from a committee of Member State representatives, and submit the final texts to the European Parliament and Council for scrutiny.

This is an interesting and important time for businesses. The UK's data protection landscape is evolving significantly, with the DUAA introducing a series of legal considerations and changes over the coming year. At the same time, the EU's decision to proceed with renewing the UK's adequacy status is a positive signal for those managing cross-border data flows, that DUAA will not disturb such flows between the UK and EU.

However, carefully understanding the staged rollout of the DUAA is critical. Businesses should continue to monitor developments closely and take the opportunity to assess how the changes could affect internal processes, contracts, and risk exposure.

If your business needs guidance on the DUAA, its implications, progress or how it may impact your operations, you can contact Privacy Partnership for tailored advice and strategy planning.

You can read the EU's announcement **here** and the commencement regulations **here**.

UNITED KINGDOM

ICO PROPOSES NEW APPROACH TO SUPPORT PRIVACY-FIRST ADVERTISING

On 7 July 2025, the Information Commissioner's Office (**ICO**) launched a call for views on a proposed enforcement approach under PECR that could enable privacy-preserving alternatives to the current AdTech model. The aim is to support innovation by allowing low-risk advertising without consent, while maintaining strong protections for personal data. The ICO also updated its guidance on Storage and Access Technologies to reflect the new Data (Use and Access) Act and is commissioning user research to align regulation with public expectations. Consultations close in August and September, with final guidance due in early 2026.

You can read the ICO's announcement **here.**

ONLINE AGE CHECKS NOW MANDATORY TO PROTECT CHILDREN FROM HARMFUL CONTENT

Ofcom has begun enforcing new rules requiring tech platforms to implement effective age checks to stop children from accessing harmful online content, including pornography, self-harm and eating disorder material. Services such as Pornhub, Reddit, X, Discord, and Grindr are amongst those now deploying age assurance systems, with Ofcom vowing to investigate any non-compliant platforms. The new enforcement regime also applies to platforms that allow users to share extreme or harmful content. Ofcom's wider programme will monitor the most popular sites used by children, such as TikTok, YouTube, and Instagram - scrutinising how they manage risks, moderate content and configure algorithms. Backed by strong parental support, Ofcom has warned tech companies to prioritise safety or face regulatory action.

You can read OFCOM's announcement **here.**

SCOTTISH CHARITY FINED AFTER DESTRUCTION OF SENSITIVE ADOPTION RECORDS

On 28 July 2025, the ICO fined Scottish charity Birthlink £18,000 for the unlawful destruction of around 4,800 personal records, including irreplaceable handwritten letters and photographs from birth parents. The breach (caused by poor data protection awareness and weak records management) may have permanently erased parts of individuals' family histories. Despite internal concerns, staff continued destroying files without fully understanding what was being lost. The ICO highlighted the emotional weight of the incident, highlighting that such records could represent identity, memory, and belonging. Since the breach, Birthlink has introduced remedial steps, including appointing a Data Protection Officer and digitising remaining records.

You can read the ICO's announcement **here.**

ICO WINS TRIBUNAL RULING ON TIKTOK PENALTY APPEAL

On 8 July 2025, the ICO welcomed a First-tier Tribunal decision confirming it had legal authority to issue TikTok a £12.7 million fine in 2023. TikTok had argued the "special purposes" exemption applied to its processing, but the Tribunal found this did not cover the misuse of children's data. The case will now proceed to a full hearing on the substantive GDPR violations, with the ICO calling the decision a key step in protecting young users online.

You can read the ICO's announcement **here** and read the full judgment **here.**

ICO CONCLUDES REVIEW OF MOD BREACH AFFECTING AFGHAN APPLICANTS

On 15 July 2025, the ICO issued a statement on its oversight of the Ministry of Defence's (**MoD**) internal investigation into a 2022 data breach involving over 18,000 Afghan relocation applicants. Initially thought to impact only a small number, the breach was caused by hidden data in a shared spreadsheet. While no further regulatory action is being taken, the ICO called the incident unacceptable and emphasised the need for robust protections, particularly for vulnerable individuals. The ICO has since published a blog explaining its decision not to pursue further enforcement action following the MoD's 2022 breach exposing data of over 18,000 Afghan nationals. While acknowledging the seriousness of the incident, the ICO said the MoD had since taken significant remedial steps and expended substantial public resources to address the risks. The blog noted that further regulatory action would not add sufficient value given

the lessons already learned but reaffirmed that the breach was unacceptable and must not happen again.

You can read the ICO's announcement **here**, and the blog post **here.**

NCSC URGES ORGANISATIONS TO PREPARE FOR WINDOWS 11 MIGRATION AHEAD OF AUTUMN DEADLINE

On 24 July 2025, the UK's National Cyber Security Centre (**NCSC**) warned organisations to prioritise upgrading to Windows 11 before Windows 10 reaches end-of-life on 14 October 2025. The blog highlights the security risks of continuing with unsupported systems, noting previous attacks like WannaCry as cautionary examples. Many devices may not meet the new hardware requirements for Windows 11, including TPM 2.0 and Secure Boot, but the NCSC encourages viewing hardware replacement as a chance to boost overall cybersecurity posture. Updated configuration packs are now available to support a smoother transition.

You can read National Cyber Security Centre's announcement **here.**

UK LAUNCHES COMPUTE ROADMAP TO POWER AI BREAKTHROUGHS AND BOLSTER SCIENTIFIC DISCOVERY

On 17 July 2025, the UK government unveiled its new Compute Roadmap - a national strategy to vastly scale domestic computing power and support the country's ambition to become a global AI leader. The plan will prioritise projects aligned with national interests, such as NHS innovation and green technology, and unlock cutting-edge scientific research through a twentyfold expansion of the UK's AI Research Resource (**AIRR**).

The roadmap brings major upgrades, including the launch of Isambard-AI, one of the world's most powerful supercomputers, and the establishment of the UK's first National Supercomputing Centre in Edinburgh. With full rollout planned by 2030, AIRR will reach 420 AI exaFLOPs, equivalent to a billion people working for 13,000 years in a single second. AI Growth Zones in Scotland and Wales are also being developed to attract billions in private investment and create thousands of jobs.

The initiative marks a step-change in the UK's sovereign AI capabilities and underlines the government's ambition to be an AI maker, not just a taker. Alongside the roadmap, a dedicated AI for Science Strategy is being launched to accelerate breakthroughs in

healthcare, climate science, and materials engineering. Backed by £500 million and led by a panel of scientific and industry experts, the strategy will ensure AI is embedded into the UK's research ecosystem while upholding trust, transparency, and reproducibility.

You can read the official press release in full **here.**

UK LAUNCHES $1M AI FELLOWSHIP TO BUILD OPEN-SOURCE TOOLS FOR PUBLIC SERVICES

On 11 July 2025, the UK government announced a new Open-Source AI Fellowship, backed by a $1 million grant from Meta to the Alan Turing Institute, to embed top AI engineers within government for 12 months. The fellows will use open-source models like Llama 3.5 to develop practical tools that improve public services, reduce costs, and strengthen national security. Applications open next week, with fellowships beginning in January 2026.

Fellows will join DSIT's AI Incubator -creators of the AI assistant "Humphrey" and focus on real-world problems like language translation for national security, construction planning automation, and secure offline AI tools for emergency response. Their work will be open sourced for broader benefit and is expected to contribute to the government's Plan for Change, potentially unlocking up to £45 billion in public sector productivity.

The launch follows early success stories like "Caddy," an AI assistant developed with Citizens Advice that's now helping Cabinet Office staff speed up grant decision-making. Early pilots showed Caddy halved response times and increased staff confidence, with 80% of AI-generated answers ready for immediate use. The Fellowship aims to scale such impact across government and reinforce the UK's sovereign AI capabilities.

You can read the official press release **here.**

EUROPEAN UNION

EDPB ADOPTS HELSINKI STATEMENT TO SIMPLIFY GDPR COMPLIANCE

On 3 July 2025, the European Data Protection Board (**EDPB**) published the Helsinki Statement, setting out new steps to make GDPR compliance easier, especially for SMEs, while boosting regulatory clarity and cross-sector cooperation. The Board pledged to release

practical tools like templates, checklists and FAQs and to improve consistency by aligning national and EDPB guidance. Early engagement with stakeholders and stronger ties with non-data protection regulators will also be central to delivering more accessible and resilient data protection across Europe.

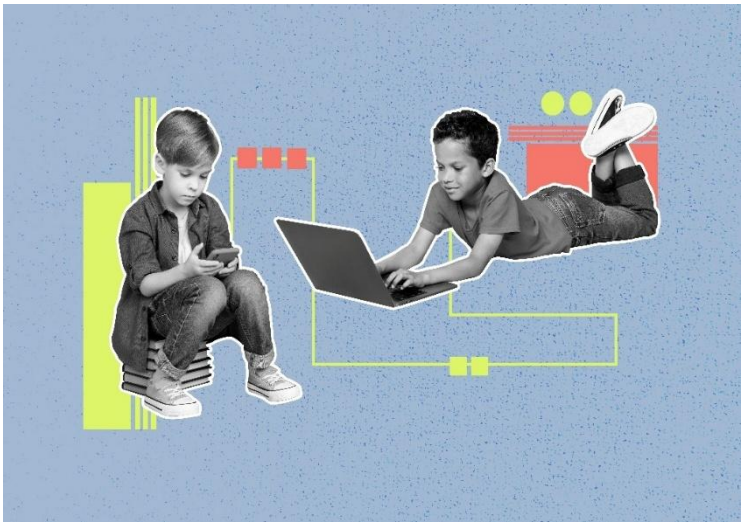
You can read the EDPB's announcement **here.**

EDPB & EDPS SUPPORT GDPR RECORD-KEEPING RELIEF FOR SMES - BUT REQUEST CLARITY

On 9 July 2025, the EDPB and European Data Protection Supervisor (EDPS) issued a Joint Opinion welcoming the European Commission's Proposal to simplify GDPR record-keeping obligations for organisations under 750 employees. The proposed changes aim to ease administrative burdens for SMEs and small mid-cap companies (**SMCs**), but the regulators urged clarification on the use of thresholds and definitions. They also called for confirmation that public bodies are excluded from the exemption and stressed that any simplification must preserve fundamental rights protections.

You can read the EDPB's announcement **here.**

EU ANNOUNCES NEW GUIDELINES AND AGE VERIFICATION BLUEPRINT TO PROTECT MINORS ONLINE



On 14 July 2025, the European Commission unveiled two major initiatives under the Digital Services Act (**DSA**) - new Guidelines on the Protection of Minors and a blueprint for age verification online. The guidelines set clear expectations for platforms to improve safety, privacy, and mental health safeguards for children, including stricter content controls and privacy-by-default settings. A pilot age verification scheme is also underway in five Member States, aiming to launch national apps by early 2026.

You can read the speech in full **here.**

EU FINALISES CODE OF PRACTICE FOR GENERAL-PURPOSE AI

On 10 July 2025, the European Commission published the final General-Purpose AI Code of Practice, developed by 13 experts with input from over 1,000 stakeholders. The voluntary Code helps model providers prepare for the AI Act's transparency, copyright, and safety rules set to apply from 2 August 2025. It includes a Model Documentation Form, copyright compliance guidance, and systemic risk mitigation practices. Providers who sign the Code will benefit from reduced admin and greater legal certainty under the AI Act.

You can read the Commission's announcement **here.**

EU HOLDS HIGH-LEVEL WORKSHOP TO STRENGTHEN STRATEGIC AUTONOMY IN AI COMPUTE STACK

On 7 July 2025, the European Commission hosted a high-level multistakeholder workshop in Brussels to discuss the future of Europe's AI compute stack. Bringing together chip designers, cloud providers, and model developers, the session aimed to boost Europe's strategic autonomy by reducing dependencies across the AI infrastructure chain. Discussions focused on scaling sovereign, co-designed systems and identifying collaborative opportunities to inform future EU policy and investment in AI compute.

You can read the Commission's announcement **here.**

EUROPEAN COMMISSION BRINGS MICROSOFT 365 USE INTO LINE WITH EU DATA PROTECTION RULES

The European Commission has successfully addressed data protection failings in its use of Microsoft 365, following enforcement action by the European Data Protection Supervisor (**EDPS**). In March 2024, the EDPS identified multiple infringements under Regulation (EU) 2018/1725, relating to purpose limitation, international transfers, and unauthorised disclosures. The Commission has since implemented updated contractual, technical and organisational measures - such as limiting data transfers, enhancing transparency, and ensuring processing only occurs on documented instructions. The EDPS has now closed the proceedings, signalling that compliance has been achieved. Other EU institutions using Microsoft 365 are encouraged to follow suit.

You can read the Commission's announcement **here.**

AUSTRIA

REMOVAL OF SIS ALERTS FOLLOWING NEGATIVE ASYLUM DECISIONS - GUIDANCE FROM THE DATA PROTECTION AUTHORITY

The Austrian Data Protection Authority (**DSB**) received numerous complaints from third-country nationals seeking the deletion of Schengen Information System alerts after receiving negative asylum decisions. Many remain in other Schengen states, prompting deletion requests. However, under Article 9 of Regulation (EU) 2018/1860, such removal requires consultation between the Member State of current residence and Austria. Without this consultation, deletion requests will be rejected. Individuals are urged to contact local immigration authorities to initiate the process properly.

You can read the DSB's announcement **here.**

AUSTRIAN DSB ISSUES GUIDANCE ON FREEDOM OF INFORMATION ACT AHEAD OF SEPTEMBER COMMENCEMENT

On 2 July 2025, the DSB announced that Austria's new Freedom of Information Act will take effect on 1 September 2025. Under Section 15 IFG, the DSB published guidelines, a circular (dated 27 June 2025) and FAQs to support institutions subject to disclosure obligations. The DSB will also evaluate the Act's application annually, with data submissions due via the Justiz-Online portal beginning in early 2026. Further details on documentation and deadlines will be shared in August 2025.

You can read the DSB's announcement **here.**

CROATIA

€370,000 IN FINES ISSUED FOR SECURITY FAILURES UNDER THE GDPR

The Croatian Data Protection Authority (**PDPA**) imposed two fines totalling €370,000 against two companies for inadequate security measures. HEP-Toplinarstvo was fined €320,000 for storing passwords in plain text, failing to implement basic security measures, and not cooperating with the regulator. A further €50,000 fine was issued to an ICT company after a hacker breached its systems,

exposing user data. The company failed to implement adequate safeguards to ensure system resilience and protect against unauthorised access. So far in 2025, the Croatian authorities have issued twelve fines amounting to €900,500.

You can read the PDPA's announcement **here** (only available in Croatian).

€350,500 IN FINES ISSUED IN CROATIA, INCLUDING €175,000 FOR SPORTSBOOK BREACH

On 2 July 2025, the Croatian PDPA announced eight new GDPR-related fines, totalling €350,500. A €175,000 fine was issued to a sports betting company for failing to implement basic security safeguards, such as encrypted connections, strong passwords, and secure data transfer protocols. The firm had also failed to delete expired user data and to back up personal data, citing cost concerns despite holding over 70,000 user profiles.

A €101,000 fine was issued to the Croatian Insurance Bureau after over one million vehicle owners' data was exposed. The PDPA found inadequate safeguards and a lack of retention limits, with the agency noting the risk of data being accessed by unauthorised persons. Other fines ranged from €2,500 to €35,000 for various GDPR violations.

You can read the PDPA's announcement **here.**

You can read this announcement **here.**

DENMARK

DANISH DIGITAL AGENCY HEAVILY CRITICISED OVER DIGITAL POST SECURITY FAILURES

On 8 July 2025, the Danish Data Protection Authority (**Datatilsynet**) issued serious criticism of the Danish Digital Agency following a series of personal data breaches linked to the rollout of the Next Generation Digital Post (**NgDP**) platform in 2022 and a subsequent update in 2023.

The breaches, reported between March 2022 and February 2023, involved issues such as unintended read access to mailboxes, data migration errors, and incorrect registration of users. Further technical problems during an August 2023 update prompted the Authority to launch its own investigation.

In its decision, the Authority stressed that the NgDP serves as a critical national communication tool between public authorities, citizens, and businesses. Given the platform's scale and legal significance, the Datatilsynet concluded that the Danish

Digital Agency failed to implement adequate technical and organisational safeguards, putting large volumes of sensitive data, and data subjects' rights at risk.

You can read the Datatilsynet's announcement **here.**

FRANCE

CNIL AND SNCF VOYAGEURS LAUNCH PRIVACY AWARENESS CAMPAIGN FOR TRAIN PASSENGERS

On 4 July 2025, the French Data Protection Authority (**CNIL**) and SNCF Voyageurs have partnered to raise awareness among the 10 million daily users of TER, Intercités, OUIGO, and TGV INOUI services about protecting their personal data while on the move.

From passengers leaving devices unlocked to password notes stuck to laptops, small lapses can pose major privacy risks. In response, the CNIL developed an educational infographic, now accessible through onboard Wi-Fi portals, offering practical tips such as:

- Using privacy screen filters
- Locking devices when unattended
- Using password managers
- Being alert to phishing attempts

Short awareness messages are also being broadcast on train screens, with full rollout continuing throughout the year. For younger travellers, the initiative includes interactive games and animated videos through the Junior & Cie service. The CNIL's card game "All together, be careful on the Internet!", initially trialled during summer 2024, has now been made a regular part of Junior & Cie activities, helping children develop good digital habits through play.

You can read the CNIL's announcement **here.**

CNIL RENAMES FORESIGHT COMMITTEE TO SCIENTIFIC AND FORESIGHT COUNCIL

On 10 July 2025 (in a move to better reflect its evolving scope and expertise) the CNIL officially renamed its "Foresight Committee" the "Scientific and Foresight Council", coinciding with the partial renewal of its members. Since 2012, this expert-led body has helped guide the CNIL's long-term thinking on emerging digital, ethical, and societal

challenges. Now under the renewed name, the council will continue to advise the CNIL three times a year, particularly supporting its Digital Innovation Laboratory (**LINC**) through experimentation, thought leadership, and contributions to its *Innovation and Foresight Notebooks*. Chaired by CNIL President Marie-Laure Denis, the council holds diverse expertise, from philosophy and sociology to design and quantum physics. It includes a mix of academics, entrepreneurs, journalists, and CNIL board members. The Council will continue its mission to inform CNIL's ethical and regulatory direction, including pressing issues like AI regulation, digital freedoms, and platform governance.

You can read the CNIL's announcement **here.**

"AUGMENTED" CAMERAS TO ESTIMATE AGE IN TOBACCO SHOPS - CNIL CLARIFIES POSITION

On 11 July 2025, the CNIL ruled that the use of AI-powered "augmented" cameras in French tobacco shops to estimate customers' ages is neither necessary nor proportionate under the GDPR. While the systems aim to help tobacconists verify age when selling restricted products like tobacco and alcohol, the CNIL found they still require manual ID checks and therefore offer no compliance advantage. Instead, they pose risks to privacy and data protection, especially given their default facial analysis of all individuals and the lack of opportunity to object. The regulator reiterated that only essential data processing is lawful and encouraged less intrusive alternatives, such as traditional ID checks or digital proof-of-age apps.

You can read the CNIL's announcement **here.**

CNIL HIGHLIGHTS THE ECONOMIC VALUE OF DPOs IN BUSINESS

On 23 July 2025, a new CNIL-backed study showed that appointing a Data Protection Officer (**DPO**) often provides measurable economic benefits, especially in companies that treat GDPR compliance as a strategic asset rather than a burden. Based on survey data from over 3,600 DPOs and follow-up interviews, the findings show that DPOs can support business growth through stronger tender performance, reduced risk of fines or data breaches, and improved data management efficiency. The CNIL noted that

organisations investing properly in the DPO role, by involving them in strategy, aligning GDPR with CSR goals, and quantifying outcomes, are those best positioned to profit from compliance. As with sustainability, it suggests the most forward-thinking firms will view privacy not as a checkbox but a value driver.

You can read the CNIL's announcement **here.**

CNIL RELEASES FINAL AI RECOMMENDATIONS AND PREVIEWS UPCOMING WORK

On 17 July 2025, the CNIL finalised its latest AI guidance, clarifying how GDPR applies to AI models trained on personal data, the security of system development, and data annotation practices. The new recommendations, developed through public consultation, include practical tools like a summary sheet and checklist to support AI developers in aligning innovation with compliance. Looking ahead, the CNIL will release further sector-specific guidance (covering education, health, and the workplace), assess stakeholder responsibilities across the AI value chain, and develop tools like PANAME to detect personal data processing in models. Ongoing research into explainable AI (**xAI**) will also inform future outputs. The work forms part of CNIL's 2025–2028 strategic plan to foster trustworthy AI in Europe.

You can read the CNIL's announcement **here.**

CNIL CLARIFIES RULES ON DETECTING ACTIVE CALLS DURING MOBILE BANKING TRANSACTIONS

On 15 July 2025, to combat fraud by manipulation where customers are pressured into authorising transactions while on a call, some banks wish for their apps to detect if a call is in progress. The CNIL has clarified that while this can help prevent scams, it must respect strict conditions - user consent is required (as per Article 82 of the French Data Protection Act), data access must be minimal (e.g. only detecting call status, not content), and alternative ways to complete transactions must be offered. Users must also be able to withdraw consent easily and stay informed of the impact on functionality. Retention of this data is limited unless anonymised, and banks must ensure transparency, privacy safeguards, and compliance with GDPR principles at every stage.

You can read the CNIL's announcement **here.**

CNIL LAUNCHES CONSULTATION ON GDPR-COMPLIANT WEB FILTERING PRACTICES

On 28 July 2025, the CNIL opened a public consultation on its draft recommendation concerning the use of web filtering gateways in professional settings. Aimed at helping organisations deploy cybersecurity tools that comply with the GDPR, the recommendation addresses the growing use of AI-driven filtering technologies designed to secure employee internet access. While such systems support data security obligations under Article 32 of the GDPR, they also involve the processing of personal data, necessitating privacy-by-design considerations. The consultation is open until 30 September 2025 and targets both data controllers and providers of filtering solutions.

You can read CNIL's announcement **here.**

GERMANY

BFDI OPENS PUBLIC CONSULTATION ON AI MODEL DATA PROTECTION

On 22 July 2025, the German Federal Commissioner for Data Protection and Freedom of Information (**BfDI**) launched a public consultation to explore how AI models, particularly Large Language Models (**LLMs**), handle personal data during training. With concerns over models reproducing personal information verbatim, the BfDI aims to gather insights from providers and researchers to shape practical and balanced regulatory guidance. The initiative seeks to increase transparency, avoid unrealistic rules, and support the development of effective data protection strategies for AI systems.

You can read the BfDI's announcement **here.**

FANPAGES CASE - COLOGNE COURT RULES AGAINST BFDI, FURTHER APPEAL UNDER CONSIDERATION

On 24 July 2025, in a key case on government use of Facebook fan pages, the Cologne Administrative Court partially overturned the BfDI's 2023 decision that banned the Federal Press Office from operating its page due to data protection concerns. While Meta's related claim was mostly dismissed, the court did not support the BfDI's full position. The regulator is now weighing an appeal. The outcome may shape how German public bodies approach social media use under joint controllership rules.

You can read the Commissioner's announcement **here.**

GERMAN DATA REGULATORS PUSH TO STREAMLINE DUAL REPORTING UNDER NIS 2 AND GDPR

In July 2025, Germany's state data protection authorities (DPA) proposed a legislative change allowing companies to report IT security incidents and data breaches through a single process. Currently, separate reports are needed under the NIS 2 Directive and the GDPR. The proposal, submitted to the Federal Ministry of the Interior, calls for a joint digital system managed by the BSI, aiming to reduce bureaucracy and speed up regulatory action when incidents involve both cybersecurity and personal data.

You can read the DPA's announcement **here**.

GERMAN DPA ACTS ON RULES AROUND NAME AND GENDER UPDATES

On 22 July 2025 (following the introduction of Germany's Self-Determination Act in November 2024) companies are now required to make it easy and free for individuals to update their first names and gender registrations. The Berlin DPA investigated a case where a web hosting provider demanded a service fee and additional paperwork before processing a name change, an approach found to breach Articles 12(2) and 16 GDPR. The company has since updated its procedures after regulatory intervention to ensure compliance.

You can read the DPA's announcement **here**.

IRELAND

IRISH DPC OPENS NEW INQUIRY INTO TIKTOK OVER STORAGE OF EEA USER DATA ON CHINESE SERVERS

On 10 July 2025, the Irish Data Protection Commission (**DPC**) launched a new inquiry into TikTok Technology Ltd after the platform admitted limited EEA user data had been stored on servers in China, contrary to previous representations. This new investigation builds on the DPC's 30 April 2025 decision, which addressed remote access to EEA data from China but not storage. The inquiry will assess TikTok's compliance with Articles 5(2), 13(1)(f), 31, and Chapter V GDPR, focusing on accountability, transparency, cooperation, and third-country transfer safeguards.

You can read the DPC's announcement **here.**

ITALY

GARANTE ISSUES EMERGENCY BLOCK ON AUTOPSY IMAGES OF CHIARA POGGI

The Garante has urgently blocked the online dissemination of autopsy images of a murder victim, labelling it a serious violation of human dignity and privacy. The video, made available online for a fee, was deemed unlawful under Italian privacy law and the Journalists' Code of Ethics. The Garante warned media and websites not to share the content and reserved the right to impose further sanctions.

You can read the Garante's announcement **here.**

ITALIAN DPA AND CARABINIERI BEGIN IMPLEMENTATION OF DATA PROTECTION AWARENESS PROTOCOL

The Garante and the Carabinieri have begun implementing their March 2025 memorandum of understanding, focused on spreading data protection awareness across Italy, particularly among youth. At a joint meeting, DPA President Pasquale Stanzione highlighted the need to educate minors on the risks and responsibilities of the digital world. Carabinieri Commander General Salvatore Luongo reiterated the force's commitment to prevention through education, especially amid growing social media exposure.

You can read the Garante's announcement **here.**

LATVIA

LATVIA'S DVI CONFIRMS CSDD'S THIRD-PARTY NOTIFICATION SERVICE IS LAWFUL UNDER THE DATA REGULATION

On 9 July 2025, following public concerns, Latvia's Data State Inspectorate (**DVI**) clarified that the Road Traffic Safety Directorate's (**CSDD**) new service, sending emails on behalf of parking providers and other partners, is lawful. The CSDD acts as an intermediary and does not transfer data to third parties. Processing is based on user consent, and recipients can opt out at any time. No third-party access to data occurs without explicit consent. The initial emails informing users about the service were deemed to be in CSDD's legitimate interest.

You can read the DVI's announcement **here.**

LITHUANIA

LITHUANIAN DPA URGES PUBLIC TO TAKE CARE WHEN SHARING DOCUMENTS ONLINE

In July 2025, The State Data Protection Inspectorate (**VDAI**) warned individuals to be cautious when uploading documents to online platforms, such as Scribd, due to risks of accidental public disclosure. Users are advised to carefully check privacy settings and terms of service before sharing personal data. The VDAI also reminded platforms of their obligations to clearly outline how user data is handled and whether it is publicly accessible. If data is published without consent, individuals should contact the platform directly or file a complaint with the VDAI.

You can read the announcement **here.**

LITHUANIA REPORTS 116 DATA BREACHES IN FIRST HALF OF 2025, MOST LINKED TO CYBER INCIDENTS

On 30 July 2025, it was reported that the VDAI received 116 reports of personal data breaches in Lithuania between January and June 2025, affecting over 168,000 individuals. Confidentiality breaches made up 86% of incidents, with 57% attributed to human error. Notably, 32% stemmed from cyberattacks, including ransomware, social engineering, and brute force access attempts, which impacted 81% of affected individuals. While 78% of incidents were reported within the GDPR's 72-hour deadline, delays remain. The VDAI imposed two fines totalling €12,529 and issued multiple corrective actions, highlighting the need for timely reporting and stronger data protection practices across sectors.

You can read the announcement **here.**

NETHERLANDS

DUTCH DPA PUBLISHES GUIDANCE ON MEANINGFUL HUMAN INTERVENTION IN ALGORITHMIC DECISIONS

On 23 July 2025, the Dutch Data Protection Authority (**AP**) released new practical guidelines to help organisations ensure meaningful human intervention in algorithmic

decision-making. This follows a recent consultation with stakeholders, including businesses and academics. The guidance is aimed at ensuring decisions (such as credit or job application outcomes) are not solely automated and are carefully reviewed by a human. The AP highlights that intervention must be real, not symbolic, and considers design, technology, process, and governance. The document clarifies that if meaningful human involvement occurs, the decision does not fall under the scope of Article 22 GDPR.

You can read the AP's announcement **here.**

DUTCH DPA - EMOTION RECOGNITION WITH AI IS 'DUBIOUS AND RISKY'

On 15 July 2025, in its latest *AI & Algorithms Netherlands Report*, the AP raised serious concerns about AI systems used to recognise human emotions. These tools, used in contexts such as customer service, smartwatches, and chatbots, are built on questionable assumptions and often lack transparency and reliability. The AP warned that such applications pose risks to human dignity and autonomy and could lead to discrimination. Chairman Aleid Wolfsen stressed that emotional expressions are neither universal nor reliably measurable using biometrics. While some emotion recognition tools will be regulated under the AI Act, the AP urged caution and called for broader ethical debate on their societal acceptability.

You can read the AP's announcement **here.**

DUTCH DPA APPROVES PROTOCOL FOR BLACKLISTING CRIMINALS FROM PORTS AND AIRPORTS

On 14 July 2025, the AP approved a protocol allowing ports, airports, and sensitive logistics hubs to deny access to individuals previously involved in serious crime at such locations, particularly drug-related offenses. Developed by the Gatekeeper Foundation, the protocol enables limited data sharing between participating sites via a central blacklist system. Individuals can be blacklisted before conviction, though stricter standards apply for inclusion in the central register versus local lists. Safeguards include a five-year data retention limit, the right to appeal, and strict access controls. The move aims to prevent criminal infiltration while maintaining GDPR compliance.

You can read the AP's announcement **here.**

DATA THEFT BY CYBERCRIMINALS DOUBLED

On 3 July 2025, the AP published its annual overview of data breaches in the Netherlands for the year 2024. The AP observed a near doubling of data theft incidents by cybercriminals in 2024, largely driven by ransomware attacks. While organisations have improved at backing up their data to avoid ransom payments, attackers have adapted by stealing personal data and threatening to publish it online unless paid, keeping their extortion model alive. The AP warned that this marks a worrying trend. Organisations are facing major financial damage, often exceeding €100,000 per incident, and are urged to improve their IT security and make secure data handling a boardroom priority. On an individual level, people are advised to be vigilant with their personal information, as stolen data can be used for scams, impersonation, or illegal activity.

You can read the AP's announcement **here.**

POLAND

POLISH COURT CONFIRMS LIMITS ON BANKS PROCESSING DATA OF FORMER AND PROSPECTIVE CUSTOMERS

On 10 July 2025, Poland's Supreme Administrative Court issued two rulings affirming the position of the Personal Data Protection Office (**UODO**) on the limits of banks' rights to retain and process data of former and potential customers. In the first case, the Court held that Santander Consumer Bank could not continue processing the personal data of a former customer based on the vague possibility of future claims. The bank had argued that its legitimate interest in potential future disputes justified retaining the data, but the Court found no actual or pending claims and ruled that speculative risks were not sufficient to justify continued processing under Article 6(1)(f) GDPR. The data must therefore be deleted. In the second case, also decided on July 10, 2025, the Court ruled in favour of the UODO against ING Bank Śląski and the Credit Information Bureau (**BIK**). The decision confirmed that personal data related to unsuccessful credit inquiries, where no agreement is concluded, must be deleted. The Court held that once the purpose of assessing creditworthiness no longer exists, there is no basis under the GDPR or Polish Banking Law to continue processing such data. The judgment reinforces that banks and credit bureaus cannot use Article 105a of the Banking Law as a blanket justification for retaining data unless an obligation or agreement has actually been formed.

You can read the UODO's announcement **here.**

POLISH DATA PROTECTION AUTHORITY URGES CLARIFICATION OF PERSONAL DATA RULES IN AIR PROTECTION PROGRAMMES

On the 0 July 2025, the President of the UODO called for an amendment to the Environmental Protection Act to address legal uncertainties about the scope of personal data that can be collected and processed in air quality programs. This followed concerns raised by local governments in the Masovian region, where a 2020 resolution implementing an air quality program lacks clarity on what personal data may be lawfully gathered. Local authorities reportedly relied on guidance from the Małopolska Voivodeship, which references using "data held by the municipality," "in-person interviews," and "social assistance data," but these terms are vague and do not guarantee a valid legal basis for processing under the GDPR. The lack of statutory authorisation in the Environmental Protection Act itself means such programmes may risk unlawfully collecting or using personal data. UODO President stressed that specific legal grounds for data collection should be embedded in the Environmental Protection Act, rather than left to lower-ranking local regulations, to prevent arbitrary data processing and ensure compliance with national and EU data protection laws.

You can read the UODO's announcement **here.**

UODO QUESTIONS SUPREME COURT OVER INADEQUATE ANONYMISATION OF HANDWRITTEN ELECTION PROTESTS

On 7 July 2025, the President of the UODO asked the Supreme Court to explain why handwritten election protest letters, potentially identifiable through handwriting, were published online despite other details being obscured. The UODO stressed that handwriting may constitute personal data under the GDPR if it can identify an individual. The Regulator has requested clarification on the Supreme Court's anonymisation procedures, whether a Data Protection Officer was involved, and what safeguards are in place for sharing content containing personal data. The UODOreminded the Court that anonymisation must ensure individuals cannot be identified, directly or indirectly, even through elements like handwriting.

You can read the UODO's announcement **here.**

UODO URGES STRONGER PRIVACY SAFEGUARDS IN POLAND'S AI DEVELOPMENT POLICY

On 28 July 2025, the UODO called for greater emphasis on privacy and data protection in the country's draft "Artificial Intelligence Development Policy" for 2030. In comments submitted to the Ministry of Digital Affairs, UODO criticised the policy's broad approach to personal data security, urging a more detailed, sector-specific framework aligned with EU laws like the GDPR and AI Act. Key proposals include recognising privacy as a cross-sectoral principle, introducing legal bases for AI use in public services, requiring fundamental rights impact assessments and publishing a comprehensive register of AI systems in public administration. The UODO also highlighted the need to address data sensitivity, open data risks and the role of independent oversight in AI governance.

You can read UODO's announcement **here.**

PORTUGAL

CNPD MARKS 30 YEARS OF DATA PROTECTION WITH SURGE IN CASES AND CALLS FOR REFORM

On 22 July 2025, Portugal's National Data Protection Commission (**CNPD**) published its 2024 Activity Report, marking its 30th anniversary and highlighting the growing complexity of data protection in the digital era. The report revealed a 216.7% rise in prior consultation requests, linked to high-risk data processing assessments under Article 36 GDPR, and a 10% increase in total cases (2,879), most of which stemmed from citizen complaints or were initiated by authorities or the CNPD itself. The CNPD issued 80 Opinions on legislation and regulation and reported 332 personal data breaches, primarily caused by human error and phishing. Enforcement included 23 fines totalling €138,375, 152 warnings, four reprimands, and a temporary processing restriction on the Worldcoin Foundation. The CNPD also celebrated its anniversary with high-profile events, including an international conference with global experts and the launch of the Lusophone Data Protection Network (**RLPD**). The Commission emphasised the need for urgent internal reform, including legislative updates and increased resources to meet the growing demands of data governance in a rapidly digitalising society.

You can read the CNPD's publication **here.**

SLOVAKIA

SLOVAKIA'S DATA PROTECTION OFFICE OPENS INTERNAL SELECTION PROCEDURE FOR SENIOR LEGAL ROLE

On 17 July 2025, the Slovak Republic's Personal Data Protection Office launched an internal selection process to fill the role of Chief State Counsellor within its Department of Administrative Procedures, based in Bratislava. The position, open to current and former civil servants across all service offices, is part of the broader efforts under Act No. 55/2017 Coll. on Civil Service. The successful candidate will lead strategic and policy-related work on national-level data protection, including oversight of compliance with the GDPR and Slovak data protection legislation. Responsibilities include conducting administrative proceedings, assessing cross-border data transfers, supervising controllers and processors, and coordinating international cooperation with EU and global bodies. The role also encompasses providing recommendations, drafting decisions, supporting certification and codes of conduct, and participating in external meetings and negotiations. Applicants must be under 65, fluent in Slovak, and meet civil service requirements, including legal knowledge and integrity. A legal background and English proficiency are preferred. All applications, including sworn declarations and qualifications, must be submitted in hard copy by July 30, 2025.

You can read the DPA's announcement **here.**

SPAIN

QUANTUM REGULATION, NEURODATA AND VULNERABILITY CLOSE OUT AEPD'S INNOVATION AND PRIVACY COURSE

On 11 July 2025, the Spanish Data Protection Agency (**AEPD**) concluded its three-day course, "Innovation and Privacy in Artificial Intelligence and Data Spaces: Building a Model Compatible with Individual Rights," held at the Menéndez Pelayo International University in Santander. The final day spotlighted regulatory challenges surrounding quantum technologies, neurodata protection, and digital vulnerability. The Deputy of the AEPD, opened with an overview of quantum technology regulation across Spain and the EU, focusing on the tension between its economic potential and cybersecurity risks. The AEPD stressed the need for post-quantum encryption standards and corporate responsibility in adopting security measures amid evolving threats. The Director of Technological Innovation at the AEPD, addressed the implications of neurotechnologies and mental data. He highlighted risks tied to biometric inferences,

such as those from eye movement or voice, and the importance of evaluating these technologies' benefits against potential harm or discrimination, particularly for vulnerable populations. The day's focus then turned to digital vulnerability. Criminologist Beatriz Izquierdo explored emerging harms involving AI-generated child pornography and deepfakes, alongside relevant legal reforms, such as Article 173 bis of Spain's draft law for protecting minors online. Political science professor Raquel Valle presented on the intersection of disability rights and AI, warning against algorithmic bias and emphasising the importance of accessible, inclusive design. In closing, AEPD President reaffirmed the agency's commitment to cross-sector collaboration and announced the return of the Agency's annual data protection session in a newly interactive format, aiming to foster dialogue among regulators, professionals, and academics.

You can read the AEPD's announcement **here.**

AEPD CAN ACT ON PROHIBITED AI SYSTEMS USING PERSONAL DATA

On 15 July 2025, Spain's AEPD confirmed it can act against AI systems that unlawfully process personal data even before the EU AI Regulation (**RIA**) fully applies. Although Spain's national AI law is not yet passed and the AEPD is not formally a market surveillance authority under the RIA, it already holds supervisory powers under data protection law. This allows it to intervene where prohibited AI systems impact privacy rights. The AEPD is reviewing its internal capacity to handle these new responsibilities and urges organisations to prepare for full RIA compliance.

You can read the AEPD's announcement **here.**

NORWAY

NORWAY BEGINS CONSULTATION ON NEW DIGITAL SERVICES ACT

On 2 July 2025, the Norwegian government published a draft Digital Services Act (**DSA**) to align national law with the EU regulation. The aim is to safeguard key rights online, including privacy, non-discrimination, and the protection of minors. The Norwegian Data Protection Authority (Datatilsynet) will oversee issues relating to personal data, such as behavioural advertising and children's online safety. The Director welcomed the proposal as a much-needed move to curb surveillance-based marketing. Other bodies, including the

National Communications Authority (**Nkom**), the Media Authority, and the Consumer Authority, will also play supervisory roles. Enforcement for very large platforms will occur at the EU level.

You can read the Datatilsynet's announcement **here.**

CANADA

POWERSCHOOL ENHANCES BREACH SAFEGUARDS AFTER CANADIAN PRIVACY ENGAGEMENT

On 22 July 2025 (following a cyberattack affecting millions across Canada) PowerSchool faced scrutiny over its data protection practices. After engaging with the Privacy Commissioner of Canada, PowerSchool has committed to bolster its security measures - such as improving monitoring and detection tools, following the breach of names, contact details, birthdates, and in some cases medical data and SINs. The federal investigation is now closed, though provincial authorities in Ontario and Alberta continue their own reviews.

You can read the OPC's announcement **here.**

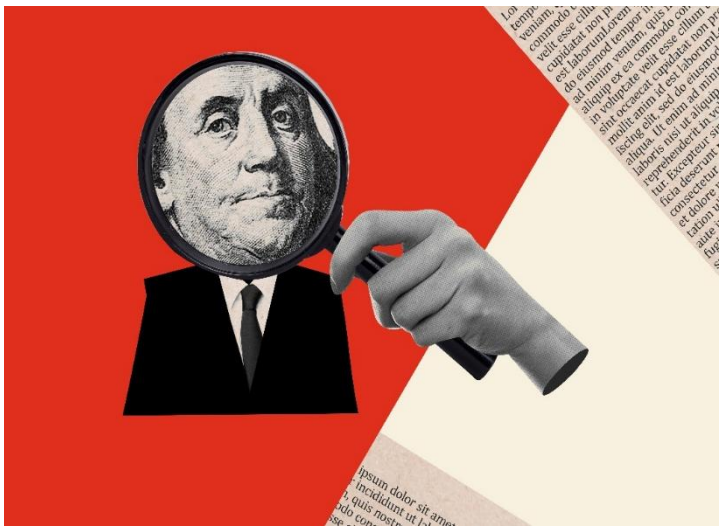
UNITED STATES OF AMERICA

TEXAS LEADS U.S. IN DATA PRIVACY ENFORCEMENT UNDER ATTORNEY GENERAL KEN PAXTON

On 21 July 2025, Texas Attorney General (**AG**) positioned the state as a national leader in digital privacy and security enforcement. Over the past year, the AG's office launched over 200 investigations into Big Tech, data brokers, automakers, and foreign entities. Key actions include record-breaking settlements with Meta ($1.4B) and Google ($1.375B), the first AI-related enforcement, and lawsuits against TikTok and General Motors. Texas also rolled out a privacy complaint portal and aggressively enforced multiple state privacy laws, including the Texas Data Privacy and Security Act.

You can read the AG's announcement **here.**

FTC RECEIVES $14.6M GRANT TO MODERNISE DATA PROCESSING FOR INVESTIGATIONS



The Federal Trade Commission secured a $14.6 million Technology Modernization Fund grant to upgrade its internal data processing systems and reduce reliance on external contractors. The funding will support the development of a cloud-based analytics platform enhanced by AI tools, enabling faster, more efficient analysis of data in fraud and antitrust investigations. By accelerating data review timelines and expanding in-house capabilities, the FTC expects to save millions while strengthening its enforcement functions. The grant aligns with federal goals to increase government efficiency and cut costs.

You can read the announcement **here.**

BEHAVIOURAL HEALTH PROVIDER DEER OAKS SETTLES HIPAA INVESTIGATION AFTER EPHI EXPOSURE

On 7 July 2025, Deer Oaks (The Behavioural Health Solution) settled with the U.S. Department of Health and Human Services' Office for Civil Rights (**OCR**) over violations of HIPAA Privacy and Security Rules. Following two incidents, including public exposure of patient data online and a ransomware breach affecting over 171,000 individuals, OCR found Deer Oaks failed to conduct a proper risk analysis. The provider will pay $225,000 and implement a two-year corrective action plan covering updated risk assessments, staff training, and new security measures to protect electronic protected health information (**ePHI**).

You can read the Department of Health's announcement **here.**

NEW YORK AND 20 STATES SUE TRUMP ADMINISTRATION OVER SNAP DATA PRIVACY DEMANDS

On 28 July 2025, New York's Attorney General (**AG**) joined a coalition of 21 attorneys general and the state of Kentucky in suing the Trump administration over its demand for states to share sensitive personal information of Supplemental Nutrition Assistance

Program (**SNAP**) recipients. The lawsuit, filed in federal court, challenges the legality of requiring states to disclose data such as Social Security numbers, addresses, and immigration statuses, information the coalition argues could be unlawfully used for immigration enforcement. The USDA's threat to withhold funding unless states comply has placed them in legal jeopardy. The suit seeks to block the policy, arguing it violates constitutional protections and federal privacy laws.

You can read the AG;s announcement **here.**

BRAZIL

BRAZIL'S ANPD HIGHLIGHTS AI AND DATA PROTECTION AT EU–LAC DIGITAL ALLIANCE SUMMIT

From 1-3 July 2025, São Paulo hosted the EU-LAC Digital Alliance High-Level Policy Dialogue to advance cooperation between Latin America, the Caribbean, and the EU on digital governance. On day one, Brazil's National Data Protection Authority (**ANPD**) took part in a panel on AI and personal data. ANPD CEO Waldemar Gonçalves emphasised the authority's role in shaping AI legislation, aligning it with Brazil's LGPD to safeguard rights like challenging automated decisions. He highlighted initiatives such as the AI Regulatory Sandbox, Technological Radar on generative AI, and recent public consultations as examples of Brazil's commitment to ethical, rights-based innovation.

You can read the ANPD's announcement **here.**

BRAZIL'S ANPD PROBES HAVAN FOR SHARING THEFT SUSPECT VIDEOS ON SOCIAL MEDIA

On 25 July 2025, the ANPD announced that it is investigating retail chain Havan over its practice of publicly posting videos of alleged shoplifters on social media. The inquiry follows a referral from the Santa Catarina Public Prosecutor's Office and focuses on possible violations of the LGPD, particularly the processing of sensitive data and risks to children's rights. In June 2025, the ANPD issued a preventive order requiring Havan to suspend video dissemination during the investigation. While no penalties have been issued, the authority stressed that surveillance and sharing evidence with law enforcement remain permitted. Havan has paused the videos voluntarily and reaffirmed its commitment to data protection as the review continues.

You can read the ANPD's announcement **here.**

CHINA

CHINA CRACKS DOWN ON 3,000 FAKE ONLINE ACCOUNTS IMITATING OFFICIAL BODIES

On 11 July 2025, Chinese authorities shut down 3,008 fake online accounts that falsely posed as media outlets, government bodies, or official live streamers to spread disinformation, peddle counterfeit goods and disrupt public order. Examples include "Dynamic News" mimicking real news organisations, and "Anhui Provincial Education Examination" impersonating state institutions to promote tutoring services. The Chinese Cyberspace Administration (**CAC**) has urged platforms to tighten account verification and pledged continued enforcement under the Internet User Account Information Management Regulations to uphold a safe and truthful online environment.

You can read the CAC's announcement **here.**

CHINA RELEASES 2024 NATIONAL INFORMATIZATION DEVELOPMENT REPORT, EMPHASISING CYBER POWER GOALS

On 30July 2025, at a press conference in Beijing, Chinese authorities unveiled the National Informatisation Development Report (2024), marking a decade since the country set its cyber power strategy and 30 years of full internet access. The report highlights significant progress in innovation, inclusivity, security, and open development - crediting informatisation with boosting public services, economic growth, and national governance. Survey data suggests citizens and companies alike see growing value in digital transformation. Looking ahead, 2025, the final year of the 14th Five-Year Plan, will focus on deepening reforms, accelerating self-reliant tech innovation, fostering equitable access, and enhancing global digital cooperation, guided by Xi Jinping's strategic vision for cyberspace.

You can read the CAC's announcement **here.**

HONG KONG

HONG KONG AND MACAO SIGN DATA PRIVACY MOU TO BOOST GREATER BAY AREA DEVELOPMENT

On 15 July 2025, Hong Kong's Privacy Commissioner for Personal Data (**PCPD**) and Macao's Personal Data Protection Bureau (**PDPB**) signed a Memorandum of Understanding to strengthen cooperation on data privacy. The agreement covers joint enforcement, mutual assistance in investigations, and efforts to enable safe cross-border data flows in the Greater Bay Area. The move aims to support digital economy growth while safeguarding personal data, reinforcing both cities' roles in regional integration and innovation.

You can read the PCPD's announcement **here.**

SOUTH KOREA

SOUTH KOREA LAUNCHES STUDENT MONITORING GROUP TO TACKLE ILLEGAL PERSONAL DATA DISTRIBUTION

On 18 July 2025, the Personal Information Protection Commission (**PIPC**) and Korea Internet & Security Agency launched a university student-led monitoring group to combat illegal personal data distribution online. Fifty students from 33 universities will monitor social platforms and digital services from July to December 2025, identifying privacy breaches and vulnerabilities. Alongside hands-on monitoring, students will attend lectures, visit related agencies, and participate in campaigns. Top participants will receive formal awards, with officials hoping the initiative fosters the next generation of data privacy experts.

You can read the PIPC's announcement **here.**

SOUTH KOREA'S PRIVACY COMMISSION URGES SUPER APPS TO STRENGTHEN DATA CONTROLS AFTER PRELIMINARY INSPECTION

On 23 July 2025, the PIPC announced findings from a preliminary inspection into five major super apps - KakaoTalk, Naver, Coupang, Baedal Minjok and Carrot - raising concerns over the opaque flow of user data. The Commission urged platforms to improve internal controls over data transfers via APIs and data warehouses, requiring oversight by privacy departments and proper access log retention. It also called for

transparency in consent practices and recommended that users be clearly informed of service terms, given the option to withdraw from individual services, and offered easy tools for managing their data rights.

You can read the PIPC's announcement **here.**

KOREA LEADS APEC WORKSHOP ON CHILDREN'S DATA PRIVACY IN DIGITAL AGE

The Personal Information Protection Commission and Korea Internet & Security Agency hosted a workshop during APEC's Senior Officials' Meeting to advance privacy protections for children and adolescents across the Asia-Pacific. Experts from 21 member economies, industry, and civil society shared insights on mandatory age verification, age-appropriate design, and safeguarding children from online harms like targeted ads and deepfakes. Key contributions came from the 5Rights Foundation and Google, both emphasising privacy-by-design principles and respect for developmental stages. The workshop builds on Korea's 2025 chairmanship of APEC and will inform regional policy recommendations to be published by year-end.

You can read PIPC's announcement **here.**

SOUTH KOREANS WANT STRONGER PRIVACY SAFEGUARDS IN AI ERA

To mark its 5th anniversary, South Korea's Personal Information Protection Commission released survey results showing that 92.4% of respondents view privacy as important, and 87.9% believe the Commission's role should be strengthened - especially considering emerging technologies like AI. The top future priority identified by the public was strengthening personal information protections related to new technologies. The Commission was also widely recognised for its enforcement actions and support for AI-related policy development, with citizens calling for continued efforts to adapt privacy protections to the changing digital landscape.

You can read the PIPC's announcement **here.**

AUSTRALIA

OAIC CONFIRMS QANTAS NOTIFIED OF ELIGIBLE DATA BREACH UNDER AUSTRALIA'S NDB SCHEME

On 2 July 2025, the Office of the Australian Information Commissioner (**OAIC**) confirmed that Qantas notified it of an eligible data breach under the Notifiable Data Breaches (**NDB**) scheme following a recent cyberattack. The OAIC is actively engaging with Qantas to ensure compliance with its NDB obligations. Qantas is also working with national cyber security agencies, police, and external experts. Affected individuals are advised to first contact Qantas directly via its support channels before escalating complaints to the OAIC after allowing the company at least 30 days to respond, in accordance with the Privacy Act.

You can read the ACMA's announcement **here.**