Privacy Partnership

JUNE NEWSLETTER

INSIDE THIS ISSUE

UK PARLIAMENT APPROVES DATA (USE AND ACCESS) ACT, SIGNALLING A SHIFT IN UK DATA GOVERNANCE

The UK Parliament has passed the Data (Use and Access) Act, with Royal Assent obtained on 19 June 2025. While the Act encountered delays during its final stages, primarily over contentious provisions related to AI model training and copyright, it ultimately secured cross-party backing.

Though the legislation introduces a range of changes, it stops short of the sweeping reform agenda previously pursued by the Conservative government. The foundations of the UK's current data protection regime remain largely intact, with the Act seen more as a recalibration than a departure from the UK GDPR framework.

One notable structural change is the planned creation of a statutory Information Commission, which will replace the individual role of the Information Commissioner. This move aims to bring greater continuity and institutional resilience, ensuring a more consistent regulatory approach over time, particularly when leadership changes.

Nicola McKilligan, Director at Privacy Partnership, commented:

"This Act marks a technical but significant shift. It refines the UK's approach to areas like automated decision-making, legitimate interests, and cookie rules—providing more clarity for organisations without

PRIVACY PARTNERSHIP

dismantling core privacy rights. The shift to an Information Commission is especially important, as it supports stability and consistent enforcement as regulatory priorities evolve."

Industry groups have welcomed clearer guidance on the use of legitimate interests and the extension of soft opt-in provisions to charities. However, critics in the EU have warned that the reforms could erode individual privacy rights and urged the European Commission to scrutinise the UK's adequacy status when it comes up for review later this year.

You can read the Government's announcement **here**, and keep updated with the Act **here**.

UNITED KINGDOM

UK REGULATOR LOOKS TO ENSURE CUSTOMER PROTECTION OVER 23ANDME BANKRUPTCY FILING

On 1 May 2025, the UK Information Commissioner's Office (**ICO**) alongside the Privacy Commissioner of Canada (**OPC**) issued a joint letter to the US Trustee addressing the need for 23andMe and any potential buyer to comply with the UK GDPR and Canada's state privacy law during the bankruptcy proceeding. The regulators warned that they may take enforcement action if they find that personal data is not adequately protected. A Consumer Privacy Ombudsman has been appointed in the US to oversee the company's handling of personal data, and the ICO and OPC have expressed their intent to engage with the Ombudsman. This follows the ICO and OPC joint investigation into the data breach at 23andMe following a cyberattack.

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

ICO RESPONDS TO RECENT CYBER ATTACKS

On 2 May 2025, the ICO produced a statement that an investigation is underway following cyber-attacks on Marks and Spencer Plc and the Co-Op Group. The ICO and the National Cyber Security Centre are collectively making enquiries into the matter to ensure a consistent approach. The ICO encourages customers who are concerned about their personal data to visit their website for guidance. Key advice includes using strong, unique passwords and monitoring official updates from affected organisations.

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

OFCOM INVESTIGATES TWO SITES OVER FAILURES TO IMPLEMENT AGE VERIFICATION MEASURES

On 9 May 2025, the UK's Office of Communications, Ofcom, announced that it has begun an investigation into two pornographic website providers, Itai Tech Ltd and Score Internet Group LLC for their failures to implement appropriate and effective age assurance systems. Ofcom has asked for information regarding their plans to comply with the Online Safety Act (**OSA**), timeline for doing so and a contact point. This continues Ofcom's implementation of the OSA which require platforms to implement effective age verification checks by July.

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

OFCOM INVESTIGATES KICK ONLINE ENTERTAINMENT FOR POTENTIAL OSA VIOLATIONS

On 14 May 2025, Ofcom launched two investigations into Kick Online Entertainment S.A. (the provider of pornography website Motherless.com) to assess whether the company conducted the required illegal content risk assessment under the Online Safety Act (**OSA**) and whether it failed in its duties for not responding to a statutory information request that was made by Ofcom. Ofcom has also received complaints that illegal content such as children sexual abuse material and extreme pornography is accessible on the site, prompting Ofcom to examine whether the appropriate safety measures are in place for UK users. This forms part of Ofcom's wider enforcement efforts under the OSA, which include actions against child abuse imagery, age assurance failures, and harmful online forums. If Kick Online is found to be in violation Ofcom may impose fines.

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

ICO FINES SOLE TRADER £50,000 FOR UNLAWFUL MARKETING CALLS

On 15 May 2025, the ICO found that a sole trader in Newcastle unlawfully made over 194,000 marketing calls to individuals who had registered on the Telephone Preference Service (**TPS**). This breached UK direct marketing laws, which prohibit the making of such calls to those on the TPS unless they have provided their explicit consent. The ICO therefore found that the sole trader failed to take appropriate and reasonable steps to comply with the law. The complaints made to the ICO also revealed that the trader was misrepresenting themselves as an affiliate to a government scheme.

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

LONDON COUNCIL REPRIMANDED BY ICO FOR DISCLOSING PERSONAL DATA

On 21 May 2025, the ICO reprimanded the London Borough of Hammersmith and Fulham Council for exposing personal data of around 6,500 people (including children) for a period of 2 years. An excel spreadsheet which was published on the WhatDoTheyKnow.com website and the Council's website as part of a freedom of information request, which included 35 hidden workbooks. After being informed (2 years later) the information was removed by the Council from both websites. The ICO has issued several recommendations, including that the Council trains its staff.

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

OFCOM IDENTIFIES CHALLENGES IN TACKLING ONLINE MISINFORMATION AND DISINFORMATION

On 27 May 2025, Ofcom posted a blog post highlighting the key challenges people have in identifying false information which include information overload, mistrust of AI, misleading data use, language and cultural differences, and limited critical evaluation skills. Emotional and social factors, such as fear of isolation or identity loss, make it difficult for individuals to disengage from misleading content or communities. Effective public messaging should be non-judgemental, use diverse communication channels, and promote tools and benefits of critical thinking and varied perspectives.

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

ICO REPRIMANDS GREATER MANCHESTER POLICE FOR MISHANDLING OF CCTV FOOTAGE

On 29 May 2025, the ICO reprimanded Greater Manchester Police after identifying serious failings in their handling and storage of CCTV footage. The investigation found that two hours of footage from a 48-hour custody period in February 2021 went missing and could not be recovered, despite internal requests to retain it and later subject access requests. The police force self-reported the breach in September 2023. The ICO's investigation found that the police force failed to protect this sensitive personal data and lacked adequate internal policies, procedures, and clarity around responsibility for quality checks. The police force has since upgraded its CCTV infrastructure and systems, introduced stricter retention and access policies, and improved internal oversight. The Independent Office for Police Conduct is conducting a wider investigation.

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

UK AI SECURITY INSTITUTE PUBLISHES PAPER ON EVAULATING AI SAFEGUARDS

On 29 May 2025, the UK AI Security Institute (**AISI**) published a research paper assessing how organisations can evaluate safeguards in advanced AI models and how this can be made practical for developers. The AISI highlights the growing importance of evaluating safeguards, such as technical measures to prevent harmful AI outputs. It is important that organisations ensure proper safeguards are in place given the increase of AI systems becoming more advanced.

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

ADA LOVELACE INSTITUTE CALLS ON GOVERNMENT TO CONTROL USE OF BIOMETRICS SURVEILLANCE

On 29 May 2025, The Ada Lovelace Institute (**the Institute**) called for the government to control the use of facial recognition technologies, following the UK's widespread use of facial recognition and biometric surveillance technologies. The Institute claims that such use is taking place in "a legal grey area" due to inadequate and fragmented governance. Despite growing deployments in policing (with the Metropolitan Police having scanned over 800,000 people's faces since 2020) schools for cashless payments, shops, and public transport, the Institute argues that there appears to be no specific legal framework to govern the use of such technologies, raising concerns about legality, public trust, and human rights. The Institute calls on the government for urgent "risk-based legislation" and the creation of an independent regulator to enforce tiered obligations based on the potential risks of each system. Without this, the Institute argues that the UK remains unprepared for the growing use of invasive technologies and will fall below the standards set by the UK courts such as the case of *Bridges v South Wales Police*.

You can read the ADA Lovelace Institute's announcement **here**.

ICO UPDATES GUIDANCE ON ENCRYPTION

On 13 May 2025, the ICO updated its guidance on encryption to reflect the regulator's "must, should, could" framework. This provides clearer guidance to organisations on what the UK regulator expects them to implement within their organisational and technical measures.

You can read the ICO's updated guidance **here**.

EUROPEAN UNION

EUROPEAN COMMISSION LAUNCHES CONSULTATION ON GUIDELINES TO PROTECT CHILDREN UNDER DSA

On 13 May 2025, the European Commission announced that it launched a public consultation on drafting guidelines to protect children's online safety under the Digital Services Act (**DSA**). To create a safe environment for children online, the Commission (alongside youth ambassadors) has drafted guidelines which include age verification, safer content recommendations, default privacy settings, child-friendly content moderation, and internal governance practices. The guidelines apply to all platforms accessible to minors, except micro and small enterprises. Stakeholders can provide feedback until 10 June 2025, with the final adoption of the guidelines expected before summer.

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

EDPB SUPPORTS COMMISSIONS DRAFT ADEQUACY DECISION FOR EUROPEAN PATENT ORGANISATION

On 6 May 2025, the European Data Protection Board (**EDPB**) announced its support for the European Commission's draft adequacy decision that would allow for transfers of data to the European Patent Organisation (**EPO**). In doing so, it published its Opinion. The EDPB found that EPO's data protection framework is largely aligned with the EU's GDPR standards. This adequacy decision marks the first time an international organisation (rather than a country or region) has been deemed as adequate. The EDPB endorsed a 6-month extension of the UK's GDPR and Law Enforcement Directive adequacy decisions (now valid until 27 December 2025) due to pending UK data protection reforms. The Board reiterated that the extension is temporary and urged the Commission to monitor legal developments in the UK, reaffirming past opinions as a reference for future assessments.

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

EU COMMISSION DEFINES AI LITERACY IN NEWLY PUBLISHED FAQS

On 7 May 2025, the European Commission published FAQs around the requirements for organisations to roll out AI literacy training for staff and stakeholders, who use AI on their behalf, to comply with the EU AI Act. This aims to make clear to organisations what is AI literacy is, how they can comply and offers information regarding

enforcement of this requirement. The FAQs also include the AI Office's approach to AI literacy.

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

EDPB AND EDPS COMMENTS ON REFORMS TO GDPR

On 8 May 2025, the EDPB and the European Data Protection Supervisor (**EDPS**) submitted a letter to the European Commission announcing their support for the proposed simplification of GDPR's Article 30(5) which relates to the record-keeping obligations. The proposed simplification would ease compliance for smaller organisations without undermining the core responsibilities, by maintaining all other GDPR obligations for controllers and processors which would remain unaffected. The letter has asked the Commission to thoroughly assess the proposal's impact on affected organisations and ensure a fair balance between data protection and the operational interests of organisations with fewer than 500 employees.

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

COMMISSION ISSUES GUIDELINES ON PROTECTING MINORS UNDER DSA

On 13 May 2025, the European Commission released draft guidelines to help platforms comply with the Digital Services Act (**DSA**) by enhancing the privacy and safety of minors online. The guidelines target platforms, although exclude micro and small enterprises, and include the need for platforms to implement age-appropriate defaults and protective features (such as private profiles, age assurance tools, and safer content recommendations). The guidelines were open for public feedback until 10 June 2025, with the final guidelines expected by summer 2025. In addition, the Commission is developing an age-verification app and a proposal for a Digital Fairness Act to further strengthen children's digital rights.

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

EU COMMISSION PROPOSES EASING GDPR RECORD-KEEPING RULES FOR SMALLER BUSINESSES

On 21 May 2025, the European Commission introduced a set of proposed amendments to the GDPR which aim to reduce compliance obligations for smaller and mid-sized enterprises. The initiative forms part of a broader regulatory simplification package intended to cut red tape for businesses while still upholding core data protection principles. A major element of the reform focuses on the record of

processing activities (**RoPA**) under Article 30 GDPR. Currently, organisations with more than 250 employees must maintain detailed documentation of their data processing unless certain exemption conditions apply. The Commission's proposal raises that threshold to 750 employees and limits the obligation to situations where data processing presents a high risk or involves sensitive categories of data.

The goal is to reduce the administrative burden on organisations that do not engage in complex or invasive processing, but still ensuring appropriate documentation where risk remains significant.

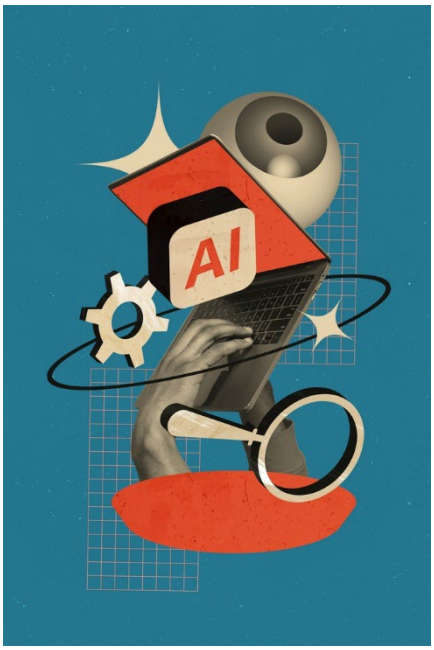
You can read the announcement **here**.

COMMISSION INVESTIGATIONS PLATFORMS FOR BREACHES OF DSA

On 27 May 2025, the European Commission announced that it has begun its formal proceedings against Pornhub, Stripchat, XNXX, and XVideos for suspected violations of the DSA. The investigation focuses on the measures these platforms have taken to protect minors and the potential risks, highlighting the platforms' lack of effective age verification and inadequate risk mitigation measures related to children's rights and well-being. EU Member States are also coordinating action against smaller pornographic sites. These steps aim to ensure minors are protected from harmful content online, reinforcing the DSA's goal of creating a safer online environment for children across all platform sizes.

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

COMMISSION SEEKS FEEDBACK INTO USE OF DATA TO DEVELOP AI



On 23 May 2025, the European Commission launched a public consultation to gather views and opinions on the use of data in AI, simplifying the current rules that apply to data and cross border data flows. The feedback received will guide the upcoming Data Union Strategy, aimed at building high-quality and trustworthy datasets essential for AI innovation in the EU. Stakeholders (including researchers, academia, and industry) are invited to submit feedback by 18 July 2025, helping position Europe as a leader in trustworthy AI.

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

EU AND SOUTH KOREA COLLABORATE TO IMPROVE CYBER COOPERATION AT SEVENTH CYBER DIALOGUE

On 20 May 2025, the EU and South Korea held their seventh Cyber Dialogue in Seoul to improve collaboration on cyber threats, security, and resilience. Officials from both sides exchanged updates on cyber policy developments and frameworks to counter cyber threats, and discussed international efforts on cybercrime, cyber capacity building and cooperation within the UN's Open-Ended Working Group on Information and Communication Technology (**OEWG**). The dialogue demonstrated the authorities' shared commitments to cyber stability and highlighted joint engagement in initiatives such as the Counter Ransomware Initiative.

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

OPINION ON EU REGULATION ON RETURNING ILLEGAL MIGRANTS PUBLISHED BY EDPS WARNS OF DATA PROTECTION OBLIGATIONS

On 28 May 2025, the EDPS published an Opinion on the EU Proposal to establish a common system for returning illegal migrants who stay within the EU. The aim of the Proposal is to streamline and provide a unified approach on the returning of illegal migrants across Member States. The EDPS reminds member states of the need for data protection safeguards to be taken, calling for thorough fundamental rights impact assessment to be conducted. In addition, the EDPS has made specific recommendations to ensure the Proposal respects individuals' rights to privacy and data protection. The EDPS highlights concern around transparency regarding the decisions to return an individual, the safeguards needed for data transfers, specifically when processing data involving children and criminal records, and ensuring the rules are consistent with existing EU data protection laws.

You can read the EDPS' announcement **here** and **here**.

DENMARK

DANISH REGULATORS ISSUE JOINT GUIDE ON COOKIE COMPLAINCE

On 15 May 2025, Denmark's Data Protection Authority (the **Datatilsynet**) and the Agency for Digitisation published a joint guide aimed at helping organisations navigate the intersection of cookie use and data protection rules. The guide targets website and app providers and identifies key

requirements under the Cookie Order and GDPR. The initiative by the regulators intends to promote a uniform understanding of the rules around cookies and clarify when each regulation applies, to ensure lawful processing of personal data.

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

DATAILSYNET UPDATES DATA BREACH GUIDANCE

On 20 May 2025, the Datatilsynet published its updated guidance on handling personal data breaches, including sections on breach notification to the Datatilsynet and affected individuals. This follows earlier guidelines which introduced examples illustrating what constitutes a personal data breach.

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

NORDIC DATA PROTECTION AUTHORITIES MET UP TO DISCUSS KEY CHALLENGES

In May 2025, the Nordic Data Protection Authorities (**DPAs**) met in the Faroe Islands, as part of their initiative to share experiences and allow for cross-border cooperation. Key themes of focus were the use of AI in law enforcement, the need for DPAs to jointly improve IT security measures and response procedures when reacting to security breaches. The meeting highlighted the need for clearer orders and appropriate resources to meet the growing demands of data protection regulation. The DPAs also discussed the handling of children's data, emphasising the need for this to remain a consistent priority throughout the DPAs agenda.

You can read the Datatilsynet's announcement **here**, and the Statement **here**.

ESTONIA

ESTIONIA DATA PROTECTION INSPECTORATE COLLABORATES ON TWO WORKING PAPERS AROUND NEURODATA AND LLMS

On 27 May 2025, the Estonian Data protection Inspectorate (**AKI**), as a member of the International Working Group on Data Protection in Technology, published two working papers. The first concerns neurodata and data protection and provides detailed insight into the data protection risks arising from the use of neurodata and neurotechnologies, often of a highly sensitive nature. The second paper discusses large language models

(**LLMs**), its development, and the data protection risks involved especially around algorithmic bias, disinformation and lack of transparency.

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

FRANCE

FRANCE DATA PROTECTION AUTHORITY FINES CALOGA FOR FAILING TO OBTAIN CONSENT FOR MARKETING

On 27 May 2025, the French Data Protection Authority (**CNIL**) fined Caloga €80,000 for its failure to obtain valid and informed consent, resulting in unlawful email marketing communications being sent. Caloga used personal data collected from brokers to facilitate email marketing campaigns it conducted on behalf of its clients. The CNIL's investigation revealed that the forms used by data brokers to collect consent were misleading, using certain display features to prompt individuals to accept marketing communication. This prevented users from being able to make a free and unambiguous decision to agree to such marketing communications. Caloga has a responsibility to ensure that the data it collects from brokers is obtained legally and that valid consent is sought. It was also found that Caloga's system made it difficult for users to withdrawal their consent easily and that the business retained data for longer than necessary.

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

CNIL FINES SOLOCAL MARKETING SERVICES €900,000 FOR UNLAWFUL DATA COLLECTION

On 15 May 2025, the CNIL imposed a €900,000 fine on Solocal Marketing Services - a company which obtained data from data brokers and then conducted commercial marketing via SMS and email without valid consent, as well as unlawfully sharing such personal data with its third-party customers. The data brokers were found to have used misleading forms which failed to meet GDPR standards for freely given and unambiguous consent. It also found that SOLOCAL was unable to demonstrate that they had obtained appropriate consent and noted the company continued to process data obtained for 17 months after finding out that proof of consent was not provided. In addition, an injunction was imposed on the company to stop using the data, and a €10,000 daily penalty was imposed for continued non-compliance after a 9-month grace period.

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

CONSULTATION LAUNCHED ON CNIL'S DRAFT REFERENCE FRAMEWORK

On 23 May 2025, CNIL announced that it launched a public consultation on its draft reference framework on the provision and granting of credit within the financial sector. The framework is aimed at improving transparency and data protection compliance under GDPR during the assessment of creditworthiness, which requires processing personal data. This is aimed at loan companies following growing use of automated decision making and AI in the sector. The reference framework provides comprehensive recommendations on common practices. Open until 18 July 2025, the CNIL invites stakeholders such as credit institutions, brokers and civil society to participate.

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

CNIL IMPOSES 10 SANCTIONS FOR BREACHES OF GDPR

Since the beginning of this year, CNIL has issued 10 sanctions under the simplified procedure, totalling €104,000, for violations of the GDPR. Six sanctions were due to unlawful surveillance of employees, including excessive video surveillance and constant geolocation tracking of vehicles. The CNIL found that in these instances monitoring was not justified by security needs or theft prevention, retained for longer than necessary, and there was a lack of transparency.

The CNIL found that a dating site had failed to report that is had suffered data breach to the CNIL, nor did it inform data subjects as required given the breach was likely to cause a high risk to the individuals' rights and freedoms.

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

CNIL PUBLISHES TWO NEW GUIDES ON DATA BREACHES FOR SCHOOLS

On 15 May 2025, the CNIL publishes two new guides on data breaches for the education sector to help manage personal data breaches. Given that schools are processing large amounts of personal data, the CNIL has published this guide for support, with one guide for data protection officers and the other for staff. The guides detail what a data breach is, outline obligations for responding, and outlines security measures. Practical examples of real-world scenarios are included, in addition to guidance around five common situations that result in a breach.

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

CNIL REMINDS RETAILERS OF SHOPPERS RIGHTS WHEN USINGSELF CHECKOUT AUGMENTED CAMERAS

On 6 May 2025, the CNIL published guidance on retailers deploying augmented cameras at self-checkouts and the implications this has on data protection rights. Retailers are using such cameras to help detect errors or theft, with such systems able to analyse real-time video to monitor shopper's scanning behaviour. These cameras collect personal data and are generally not anonymous meaning GDPR rules apply. The CNIL reminded retailers that such systems must comply with GDPR principles, including transparency, data minimisation, and the need to respect individuals' rights requests. The CNIL recommended retailers investigate less intrusive alternatives where possible and ensure that their use of augmented cameras does not disproportionately infringe on the rights and freedoms of shoppers.

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

GERMANY

HAMBURG HMBBFDI DECIDED NOT TO TAKE ACTION AGAINST META FOR ITS AI TRAINING

On 27 May 2025, Hamburg Data Protection Authority (**HmbBfDI**), together with other German Data Protection Authorities, decided not to issue a national provisional injunction against Meta regarding its AI training using social network user data. This decision (following a recent ruling by the Cologne Higher Regional Court) emphasised the need for a consistent European approach. With an EU-wide evaluation of Meta's practices forthcoming, the authorities consider a single-country injunction unsuitable for addressing the broader issue across Europe.

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

LOWER SAXONY DPA SUCCESSFUL OVER REJECT ALL COOKIES BUTTON

On 20 May 2025, the State Commissioner for Data Protection of Lower Saxony (**DPA**) secured a court ruling by the Administrative Court of Hanover that now requires websites to offer a clearly visible "Reject All" button alongside "Accept All" on cookie consent banners, to ensure genuine user choice. This follows a complaint against a media house whose manipulative banner design (which made rejecting non-essential cookies difficult and made consent unclear) violated the GDPR and national data

protection laws. The Administrative Court highlighted multiple violations, including the use of misleading labels and obscuring of the information, confirming that consent was neither informed nor voluntary. The DPA warned of the importance of this ruling in promoting privacy and urged website providers to adopt compliant consent practices.

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

IRELAND

IRISH DPC DISCUSSES META AI TRAINING

On 21 May 2025, the Irish Data Protection Commission (**DPC**) announced that it is engaging with Meta over its plans to train its AI model using public data from Facebook and Instagram adult users in the EU/EEA. After raising concerns in early 2024, the DPC requested Meta to pause its training after several concerns were raised. Meta has since collaborated with the EPDB to seek a GDPR Opinion for consistent AI data protection standards, which was issued in December 2024. Following this, Meta updated its transparency notices, objection mechanisms, and privacy safeguards and has decided to resume such AI training in May 2025. Individuals are reminded to continue to monitor their privacy settings and controls when using social media and internet platforms. The DPC will continue monitoring AI compliance to ensure responsible innovation and protection of individuals' data.

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

IRELAND'S CLASS ACTION AGAINST MICROSOFT OVER DATA BREACH

The Irish Council for Civil Liberties (**ICCL**) applied to the High Court to begin Ireland's first-class action lawsuit against Microsoft, targeting a major "Real-Time Bidding" (**RTB**) data breach in its advertising system. RTB is where advertisers compete to show ads based on users' personal information collected from websites, usually to show personalised ads based on the users' data. The lawsuit argues that Microsoft has no control over the personal data it holds once it has been made available to potential advertisers. This legal action, brought under the new EU Collective Redress Directive, aims to compel Microsoft to align its practices with the GDPR. The case could have wide-reaching implications across the European Economic Area due to Microsoft's European headquarters being in Ireland. Users of Microsoft products like Windows, Xbox, Office, Edge and platforms using Xandr advertising are among those impacted by the breach.

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

ITALY

ITALIAN GARANTE LAUNCHES CONSULTATION ON PAY OR CONSENT MODEL

On 5 May 2025, the Italian Data Protection Authority, the Garante, launched a public consultation to review the lawfulness of the "pay or consent" model. The model would allow users the ability to agree to all cookies or pay a fee to access online content. The Garante raised concerns over whether consent is truly freely given, as required under the GDPR, as users will often just accept the cookies without full understanding to avoid a payment. The consultation seeks stakeholder input on alternative solutions that balance privacy rights with publishers' economic needs instead of sanctions. The consultation remains open for 60 days since publication and the deedback will help shape fair and transparent practices.

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

GARANTE FINES ACEA ENERGIA €3 MILLION AND INVOLVED AGENCIES €850,000 FOR UNLAWFUL TELEMARKETING

On 7 May 2025, the Garante imposed a €3 million fine against Acea Energia and €850,000 against a network of agencies and companies that were involved in making aggressive telemarketing calls and for unlawfully processing of personal data. Investigations revealed the unlawful use of detailed user data from recent energy provider switches without consent, misleading customers with false technical issues to induce new contracts. Acea Energia ended its relationship with the implicated agency once discovering these breaches and implemented appropriate corrective measures to improve security of processing. The Garante also required Acea to notify affected individuals, review and verify current sub-processors, and stop all involved parties from using unverifiable contact lists.

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

LUKA FINED €5 MILLION FOR LACKING A LAWFUL BASIS FOR PROCESSING

On 19 May 2025, the Garante fined US-based Luka Inc. €5 million over violations of its management of the chatbot Replika, and launched a new investigation into its generative AI's data processing practices. The Garante uncovered that since February

2023, Luka failed to have a lawful basis in place for processing personal data, did not implement appropriate age verification measures (although the company claimed that it excluded minors) and had provided an inadequate privacy policy. The Garante's investigation revealed that the current age verification in place was insufficient. In addition, the Garante's new investigations requests that Luka provide detailed information on its data handling practices, information about risk assessments conducted and the measures in place to mitigate against risk related to the AI model's development and training.

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

UNLAWFUL TELEMARKETING IN REAL ESTATE SECTOR CAPTURES THE EYES OF THE GARANTE

The Garante imposed a fine on a widespread illegal telemarketing scheme in the real estate sector, fining the data supplier company €100,000 and the nine housing agencies involved up to €40,000 for using personal data unlawfully obtained through contact lists. This information was then used to make unlawful aggressive telemarketing calls to thousands via phone calls and WhatsApp. No prior consent was obtained for the processing of the personal information and the Garante prohibited any further use, ordering the deletion where the companies lacked consent. Further sanctions are expected. This highlights that agencies must ensure compliance with privacy laws, including verifying that the correct consent is given, and to respect data subjects' rights including any listed on the opt-out register.

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

LITHUANIA

COURT UPHOLDS VDAI FINE AGAINST VINTED FOR GDPR VIOLATIONS

On 30 May 2025, the Lithuanian Data Protection Inspectorate (**VDAI**) announced that the Regional Administrative Court dismissed UAB Vinted's appeal against the €2.385 million fine imposed by the VDAI for multiple GDPR breaches. The court confirmed that the VDAI acted lawfully and within its remit to impose the fine. The violations concerned failure to properly handle data erasure requests, lack of transparency, insufficient accountability measures, and the unlawful practice of "shadow blocking" users without a valid lawful basis. This ruling reinforces the importance of clear data processing policies and respect for individuals' data protection rights under the GDPR.

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

MALTA

IDPC BECOMES MARKET SURVEILLANCE AUTHORITY FOR MALTA UNDER EU AI ACT

On 15 May 2025, Malta's Information and Data Protection Commissioner (**IDPC**) announced that it will become the market surveillance authority for high-risk AI systems under the EU AI Act starting 2 August 2025. The IDPC is already responsible for fundamental rights enforcement and is expanding its capacity through legislative updates, internal expertise, and upcoming guidance for businesses. The Commissioner highlighted the need for collaboration with other national authorities and proposed creating a committee to coordinate efforts. As high-risk AI systems (those used for biometrics, employment, or law enforcement) face tighter scrutiny, the IDPC's role will be fundamental to ensuring compliance.

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

IDPC PUBLISHES FAQS ON DATA PROTECTION COMPLIANCE IN THE EMPLOYMENT SECTOR

On 30 May 2025, the IDPC published frequently asked questions (**FAQs**) addressing the obligations on employers to comply with the GDPR. Key topics include processing of biometric data, employee monitoring, medical checks, email account management and data retention.

You can read the IDPC's announcement **here**, and the FAQs **here**.

NETHERLANDS

DUTCH AP OUTLINES AIMS FOR TACKLING RESPONSIBLE USE OF AI

On 23 May 2025, the Dutch Data Protection Authority (**AP**) published its paper "Moving Forward Responsibly" which sets out a framework of aims for the safe and lawful development of generative AI, alongside draft GDPR preconditions for public consultation. Although AI has the potential to boost economic and social prosperity, the AP warns that many generative AI models have been trained using vast amounts of data, (including personal data) which may compromise legality and privacy. The AP warns over the need for proactive safeguards to protect fundamental rights, as reactive measures may be insufficient

given the rapid pace of development. The AP proposes a future scenario called "Values at Work," which promotes democratic control, transparency, risk assessment, and compliance with the GDPR and AI Act.

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

DUTCH AP ANNOUNCES INVESTIGATIONS INTO MUNICIPALITIES' DATA HANDLING PRACTICES

On 13 May 2025, the Dutch Data Protection Authority (**AP**) announced its upcoming investigation into several municipalities over the coming months on a random basis to assess how they handle citizens' personal data and to provide support where needed. The AP aims to ensure that the municipalities are maintaining updated record of processing registers, conducting proper data protection impact assessments, and whether an independent Data Protection Officers has been appointed to supervise data protection governance. The AP is aiming to guide rather than penalise these local authorities, emphasising the general need for improved compliance and the protection of citizens' privacy. The initiative follows concerns noted in a 2024 sector report about municipalities' ongoing struggles with data governance and privacy protections.

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

POLAND

UODO WARNS OF RISKS IN SHARING CHILDREN'S IMAGES ONLINE

On 30 May 2025, the Polish Personal Data Protection Office (**UODO**) raised concerns about the widespread sharing of children's images online, reminding users that a child's image is personal data which needs careful legal and ethical handling. While consent is commonly bundled into broad event terms, many parents are unaware that accepting participation conditions does not constitute valid consent for image processing, especially when such consents allow unlimited, unregulated use. The UODO highlighted that GDPR allows for the withdrawal of consent at any time without penalising the child's participation. The UODO warned of serious risks that could be posed including cyberbullying, deepfakes, and exploitations, encouraging reviewing the UODO's joint guide with the Orange Foundation, "Child's image on the Internet. To publish or not?", which offers practical advice on safe image use and debunks common misconceptions.

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

SUPREME COURT UPHOLDS UODO DECISION TO CEASE BIK DATA PROCESSING

On 30 May 2025, the Polish Supreme Administrative Court upheld an order by the UODO for the Credit Information Bureau (**BIK**) to stop the processing of data of an individual who applied for but did not receive a loan. Despite the loan not being granted, BIK had retained the data for the purposes of conducting credit risk analysis and scoring model development. The Court ruled that such processing lacks legal grounds under the GDPR, especially given the loan agreement was not finalised, meaning there was no ground for the further processing of the individual's data.

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

UODO INVITES STAKEHOLDERS TO PARTICIPATE IN SURVEY ON THE RIGHT OF ERASURE

On 28 May 2025, the UODO invited data controllers to provide their feedback in a voluntary and anonymous survey as part of the EDPB's Coordinated Enforcement Framework on the right of erasure. The survey aims to determine how controllers handle data deletion requests and the ways in which relevant legal conditions and exceptions are applied. The UODO will use the findings from the survey to inform best practices, guidance, and potential follow-up actions at both national and EU levels.

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

UODO COMMENTS ON REGULATION THAT ALLOWS FOR AUDIO VIDEO RECORDINGS OF MEDICAL TREATMENT

On 22 May 2025, the UODO presented the Ministry of Health its comments on its proposed regulation on hospital treatment, raising concerns around the mandating of audio-video recordings of endometriosis treatments. The UODO stated that such proposals will interfere with the rights and freedoms of the patients involved and that such processing lacks a clear legal basis justification and does not consider the appropriate safeguards needed, especially given the sensitive nature of the procedures involved. The Ministry's failure to consider a data retention policy and conduct a data protection impact assessment further undermined the proposal's legality and proportionality.

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

UODO QUESTIONS FOOTBALL ASSOCIATION LAWFUL BASIS FOR PROCESSING IMAGES OF CHILDREN

On 19 May 2025, the UODO requested clarification from the Polish Football Association around its lawful basis for processing children's images during their participation in a tournament. The UODO's request followed multiple media reports that parents were required to give consent to process children's images to let their child enter the tournament. The UODO was concerned that the nature of consent should be of a voluntary nature and was not obtained, in addition required information as to the necessity to process such images not being provided. The UODO reminded organisations that consent must be freely given and informed, questioning whether refusal could lawfully exclude a child from participating in a tournament.

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

ROMANIA

ROMANIAN DATA PROTECTION AUTHORITY FINES AG-BROKER FOR INSUFFICIENT SECURITY

On 30 May 2025, Romania's National Supervisory Authority for Personal Data Processing (**ANSPDCP**) fined AG-BROKER ASIGURARE S.R.L approximately €5,000 for violating Article 32 of the GDPR. The investigation followed a data breach notification by the company after a cyberattack exposed sensitive customer data, including national ID numbers, names, photos, and contact details. The authority found that AG-BROKER had failed to implement adequate security measures and therefore failed to ensure confidentiality, integrity, and resilience of the data processing systems as required under the GDPR.

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

ANSPDCP FINES DATA DIGGERS FOR BREACHING THE GDPR

On 30 May 2025, the ANSPDCP announced that it imposed a €12,000 fine against Data Diggers Market Research SRL for failing to have a lawful basis for processing and for failing to be transparent about its processing activities. The ANSPDCP's investigation, triggered by complaints from two EU supervisory authorities, revealed that Data Diggers had failed to provide sufficient transparency information when processing personal data, neglected to inform data subjects at first contact and did not demonstrate a valid legal basis for processing. As the lead supervisory authority, the

ANSPDCP also ordered the company to implement regular staff training to ensure compliance with data subject rights requests and having a lawful basis.

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

SLOVENIA

HEALTHCARE WORKED FINED FOR UNLAWFUL ACCESS TO PATIENT DATA

On 19 May 2025, the Slovenian Information Commissioner (**IP**) fined an employee of a university €950 for unlawfully accessing a patient's personal data without a valid reason. The employee did not need the personal data to carry out the work required of them. Although, the healthcare professional had technical access using her password, the action breached key GDPR principles, particularly lawfulness and purpose limitation. The case reinforces that access to personal data must be strictly limited to specific tasks or purposes arising from employment duties, and that curiosity or one's personal interest regarding a patient's data does not justify such access. The Commissioner called for organisations to implement access controls, ensure regular audits take place and roll out regular training for employees, especially in healthcare settings where sensitive data is involved, and the protection of individual privacy is paramount.

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

SPAIN

AEPD FINES UNIVERSITY OVER FACIAL RECOGNITION USE IN ONLINE EXAMS

On 3 June 2025, the Spanish Data Protection Agency (**AEPD**) imposed a sanction against the Universitat Internacional Valenciana (**UIV**) for unlawfully processing students' biometric data using facial recognition technology during remote exams. The AEPD's investigation concluded that such processing lacked a valid legal basis under Article 9 of the GDPR. The university had implemented a mandatory AI-based monitoring system without offering students a meaningful alternative, which means consent was unable to be freely given, and therefore invalid. The AEPD rejected the school claims that such processing was necessary for the reasons of "public interest," stating that no specific national law currently allows such biometric processing in education. While not ruling out future use of these technologies, the AEPD called for the need for a clear legislation which expresses that essential public interest can be relied upon for the "purposes of

preventing academic fraud" with defined safeguards and purposes, aligning with both the GDPR and AI Act requirements for high-risk systems.

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

AEPD ORDERS ENTITIES TO STOP THE UNLAWFUL PROCESSING OF SELF-EMPLOYED DATA FOR COMMERCIAL PURPOSES

On 20 May 2025, the AEPD issued several resolutions requiring the cessation and deletion of personal data that was unlawfully processed, involving self-employed entrepreneurs by Camerdata, Informa, Iberinform Internacional, and Datacentric. The personal data, originally obtained from the Spanish Chamber of Commerce's census, was used without a valid legal basis and such processing went beyond the institutional purpose for which it was published by the Chambers of Commerce (which was not intended for cheap marketing or providing an open-source database for commercial purposes). The AEPD reinforced that purpose limitation, transparency, and restricted access must govern the use of such data, rejecting any assumption of public availability or commercial reuse without express legislative authorisation.

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

SWEDEN

IMY CONCLUDES INVESTIGATION INTO HEALTHCARE CAMERA SURVEILLANCE

On 27 May 2025, the Swedish Data Protection Authority (**IMY**) concluded its investigation into a healthcare facility's camera surveillance of a toilet used for urine sampling, finding that such processing aligned with data protection laws. The investigation was initiated in response to concerns about privacy, but the IMY's review confirmed that the surveillance is justified, necessary, and proportionate to ensure patient safety (given the health risks of manipulated samples). IMY found that the facility had a valid legal basis for processing personal data and had properly informed patients in accordance with the Camera Surveillance Act. No violations of the GDPR or national surveillance laws were identified.

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

CANADA

CANADA'S OPC OPENS CONSULTATION TO IMPROVE CHILDREN'S DIGITAL PRIVACY

On 12 May 2025, the Office of the Privacy Commissioner of Canada (**OPC**) announced that it is exploring a new children's code to better protect children's personal information online. The code will provide practical guidance for organisations handling children's data to ensure adequate safeguards are in place. The OPC encourages child advocacy groups, businesses, parents, educators, guardians, to share their views. Stakeholders are invited to provide their input until 5 August 2025.

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

NOVA SCOTIA POWER INVESTIGATED BY OPC FOLLOWING DATA BREACH

On 28 May 2025, the OPC announced that it is investigating Nova Scotia Power following a data breach to ensure that the appropriate measures are being taken to respond to the incident. Nova is notifying affected individuals and offering a two-year credit monitoring service to help mitigate potential risks. The OPC recommends that the affected individuals take advantage of this credit monitoring services, update their passwords and monitor financial accounts to help mitigate the potential risk of fraud.

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

QUEBEC COMMISSION ORDER COMPANY TO LIMIT VIDEO SURVEILLANCE

On 28 May 2025, the Privacy Commission of Quebec (**CAI**) ruled that the trucking company, Crane Supply Company's, use of in-cab video surveillance did not minimise the privacy intrusion that comes with placing cameras within its vehicles. Although it acknowledged that the reasons for placing the cameras were related to the company's overall safety goals, the storage of the recordings for 14 days was deemed excessive. The Commission also ordered the company to limit footage to brief periods surrounding specific incidents, stop recording once the engine is off, and restrict

access to footage strictly to major accidents. The CAI also recommended that the company revise its dash cam policy to reflect these privacy safeguards and to destroy unnecessary recordings.

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

CAI REMINDS ORGANISATIONS OF STEPS TO DELETE DATA

On 9 May 2025, the CAI reminded organisations of the steps needed to delete and securely destroy personal data when the data no longer serves the purpose for which it was obtained. Two destructions procedures have been provided, one for companies, and one for public bodies.

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

UNITED STATES OF AMERICA

FTC CONCLUDES SETTLEMENT WITH GODADDY OVER SECURITY FAILURES

On 21 May 2025, the U.S Federal Trade Commission (**FTC**) concluded an order against GoDaddy for misleading consumers about its data security practices, resulting in several data incidents. The FTC found that GoDaddy failed to implement basic security measures such as multi-factor authentication and monitoring for threats. It was suggested that the company falsely claimed its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Framework. GoDaddy is now required to stop misrepresenting its security practices, implement a robust security program, and undergo independent third-party audits.

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

VERMONT PASSES BILL ON AGE-APPROPRIATE DESIGN CODE

On 29 May 2025, the Senate Bill 69, the Age-Appropriate Design Code Act was passed by both the Senate and House in Vermont. The bill aims to set default privacy and safety protections for users under 18. It requires online platforms to restrict certain harmful content and disable addictive features for children. It was signed by the Governor on 12 June 2025 and aims to create safer digital environments for children and minors.

You can read the Senate's announcement here and here.

NEW YORK COURT ALLOWS ATTORNEY GENERAL'S LAWSUIT AGAINST TIKTOK TO PROCEED

On 28 May 2025, the New York Attorney General (**AG**) welcomed the decision by the State Supreme Court Judge to reject TikTok's motion to dismiss the AG's lawsuit which claimed that the platform harms the mental health of young people. The lawsuit, filed in October 2024, accuses TikTok of misleading the public about its safety and contributing to youth anxiety, depression, and injuries linked to dangerous challenges. The AG warned against the ongoing mental health crisis among youth and vowed to continue holding TikTok accountable to protect young users.

You can read the AG's announcement here.

CPPA IMPOSES $345,178 FINE AGAINST TODD SNYDER FOR VIOLATIONS OF CCPA

On 6 May 2025, the California Privacy Protection Agency (**CPPA**) imposed a $345,178 fine against Todd Synder, a clothing retailer, for violating the California Consumer Privacy Act (**CCPA**). The company was found to have failed to process opt-out requests for over 40 days, required consumers to submit excessive information and improperly demanded identity verification for opting out. As part of the settlement, Todd Snyder must revise its privacy practices, properly configure consent mechanisms and provide employee training. The CPPA encouraged businesses to remain responsible for privacy compliance, regardless of the tools they use, and highlighted this enforcement as part of its broader initiative to uphold Californians' privacy rights.

You can read the CPPA's announcement here.

TEXAS AG SECURES $1.375 BILLOIN IN SETTLEMENT WITH GOOGLE OVER PRIVACY CONCERNS

On 9 May 2025, the Texas Attorney General secured $1.375 billion in a settlement with Google following its lawsuit in 2022, which argued that Google illegally tracked Texans' geolocation, incognito searches and biometric data without the user's consent.

You can read the AG's announcement here.

HHS REACHES SETTLEMENTS WITH COMSTAR OVER RANSOMWARE BREACH

On 30 May 2025, the U.S. Department of Health and Human Services (**HHS**) Office for Civil Rights (**OCR**) announced that a $75,000 settlement has been reached with Comstar, LLC, a company providing billing services for emergency ambulance services, following its potential violations of the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) Security Rule after it experienced a ransomware attack. The attack affected over 585,000 individuals' electronic protected health information. The OCR investigation discovered that Comstar failed to conduct a proper risk assessment. Comstar agreed to implement corrective measures such as conducting a full risk assessment, establishing a risk management plan, updating security policies and training staff. OCR recommends that all HIPAA-covered entities implement risk management into their operations and apply security best practices such as encryption in transit to prevent cyber threats.

You can read the HHS OCR's announcement **here**.

HHS SECURES $800,000 IN SETTLEMENT WITH BAYCARE

On 28 May 2025, the HHS OCR reached a $800,000 settlement with BayCare Health System following a complaint made about the unauthorised access to a patient's electronic protected health information. The complaint detailed that an individual, after having treatment at the company's facility, was contacted by an unknown individual and received a photo of a copy of their medical records and a video of someone scrolling through their medical information. The OCR's investigation revealed that a non-clinical former staff member from an affiliated physician's office improperly accessed and disclosed patient records, highlighting failures in BayCare's access controls and system activity monitoring. BayCare agreed to pay $800,000 after having violated the HIPAA and is required to implement corrective actions addressing risk analysis, access management, policy revisions and staff training to ensure the protection of data.

You can read the HHS OCR's announcement **here**.

BRAZIL

ANPD DISCUSSES AI GOVERNANCE AT UN AND IDP PANEL

On 28 May 2025, the Director of the Brazilian National Data Protection Authority (**ANPD**), joined by experts from the United Nations and Institute of Education, Development and Research (**IDP**), discussed effective governance measures to adopt to help protect human rights

in the increase of AI use. The ANPD highlighted the current work it has been doing in regulatory planning and establishing a new AI regulatory sandbox. It was highlighted that proper governance requires the need to conduct risk assessments, ensure transparency and accountability.

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

BRAZILIAN PROSECUTOR'S OFFICE URGES OPENAI TO WARN USERS OF PERSONAL DATA RISKS IN ITS RESPONSES

On 25 May 2025, the Brazilian Federal Public Prosecutor's Office (**MPF**) issued a formal recommendation to OpenAI urging it to implement clear warnings in its ChatGPT responses to inform users that information produced is generated by the AI model, rather than reliable sources. This followed concerns raised over the potential for AI to generate inaccurate or fabrication information (known as hallucinations) which can mislead its users and compromise key data protection principles of data quality, transparency and security. The MPF argued that OpenAI's reliance on legitimate interest does not justify the inadvertent generation of false personal data and criticises the current warning system as insufficient. OpenAI has 15 days to respond with actions taken or provide justification for non-compliance.

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

CHINA

CHINESE CYBERSPACE ADMINISTRATION STRENGTHENS OVERSIGHT OVER ALGORITHM RECOMMENDS ON SOCIAL MEDIA PLATFORMS

On 22 May 2025, the Cyberspace Administration of China (**CAC**) announced that following the launch of its action to tackle problems with online platform algorithms, major platforms such as Douyin, WeChat Channels, and Weibo have signed the "Algorithms for Good" declaration and have launched measures to improve content recommendation quality, transparency and user control. This initiative aims to help address the issues raised by the CAC on vulgar content, opinion polarisation and "information cocoons". Douyin has created a security and trust centre on its website to help improve transparency. Despite improvements, the CAC noted continued challenges due to the limited use of the new measures proposed, which affects

content quality and function adoption. As governing algorithms will be a continued area of work, the CAC will conduct regular inspections and governance upgrades to ensure proper protections are in place.

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

CAC ORDERS PLATFORMS TO STOP REMOVE ILLEGALLY OBTAINED DATA

On 27 May 2025, the CAC ordered top platforms including Weibo, Tencent, Douyin, and Baidu, to block and remove content related to doxxing - where personal information has been obtained and shared online illegally. The CAC warns of strict enforcement and platform accountability. The CAC's crackdown also looks to improve early warning systems, stronger punishments, improved user protection features, and public awareness campaigns to prevent and deter personal data leaks. Platforms are required to clean up published content on a regular basis and take down accounts or groups promoting such activities. Platforms should also make it easy for users to report doxxing practices.

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

CAC ANNOUNCES FILING REQUIREMENTS FOR USE OF FACIAL RECOGNITION TECHNOLOGY

On 30 May 2025, the CAC announced that organisations using facial recognition technology must complete mandatory filing procedures if they are to store facial data of 100,000 or more individuals, as required by the "Measures for Security Management of Face Recognition" (Order No. 19). Entities reaching this threshold before 1 June 2025 must file their application by 14 July 2025 with their local authorities. For any companies reaching this threshold after 1 June 2025, the filing must be completed within 30 days of meeting the threshold. Those companies who fail to comply risk legal penalties. The filing requirement aims to ensure that those handling biometric data can ensure its protection, promote transparency, and protect individuals' privacy rights amid growing facial recognition technology use.

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

HONG KONG

PRIVACY COMMISSIONER PUBLISHES GUIDANCE ON SAFE USE OF GENERATIVE AI

On 22 May 2025, Hong Kong's Privacy Commissioner for Personal Data (**PCPD**) published guidance titled "Companies Must Take the Initiative on Safe AI Practices" to help companies develop safe internal policies on the use of generative AI. This follows growing concerns about privacy risks and potential harm from the unregulated use of AI tools by employees. As the use of generative AI increases, improper use could pose high risks to the protection of personal data. The Commissioner's guidelines aim to help companies comply with the Personal Data (Privacy) Ordinance (**PDPO**).

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

PCPD COMPLETES COMPLIANCES CHECKS AGAINST 60 COMPANIES

On 8 May 2025, the PCPD announced that it conducted compliance checks on 60 organisations in 2025 examining their use of AI and how they comply with the requirements of the PDPO. The checks found that 80% (48 organisations) used AI within their day-to-day business operations, with half collecting personal data and implementing correct privacy notices and robust security measures. Most had AI governance structures and conducted risk assessments. No PDPO violations were found, but the PCPD warned organisations of ongoing risks to data privacy and ethics and the need to remain diligent over AI use. The PCPD encouraged organisations to make use of "Checklist of Guidelines for the Use of Generative AI by employees" to improve AI governance, conduct continuous risk assessments, train employees and maintain transparency to ensure responsible AI development and use.

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

JAPAN

JAPAN ADOPTS AI BILL TO PROMOTE RESEARCH AND DEVELOPMENT

On 28 May 2025, the House of Councillors passed the Bill on the Promotion of Research and Development and Application of Artificial Intelligence-Related Technologies. The Bill establishes a comprehensive national framework for the advancement of AI for the purposes of research and development, whilst addresses responsible AI use. The Bill

empowers the government to publicly name businesses involved in criminal misuse of AI and mandates company cooperation during investigations of serious incidents impacting citizens' rights. Japan's regulation of AI takes a softer approach, in which the Bill does not introduce penalties (to allow for AI innovation), but rather relies on other existing laws for enforcement.

You can read the Bill **here**.

SOUTH KOREA

TEMU SANCTIONED FOR UNLAWFUL TRANSFER OF DATA ACROSS BORDERS

On 20 May 2025, South Korea's Personal Information Protection Commission (**PIPC**) sanctioned Temu for multiple violations of the Personal Information Protection Act (**PIPA**), including unlawful cross-border data transfers and improper identity verification practices. Following an investigation, the PIPC imposed penalties totalling KRW 1.369 billion and a fine of KRW 17.6 million on Temu and its affiliated entities for failing to disclose data processing arrangements, supervise third-party processors and designate a domestic agent. The investigation revealed unauthorised processing of sensitive identity data from Korean sellers and failing to provide sufficient transparency information regarding data handling. The PIPC ordered corrective measures and will monitor compliance, also releasing a Chinese version of its foreign operator guidance to improve awareness of Korean privacy laws.

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

PIPC INVESTIGATING DATA BREACH AT SK TELECOM

On 19 May 2025, the PIPC launched an investigation into a data breach at SK Telecom Co Ltd, forming a dedicated task force under the Personal Information Protection Act. Following an emergency committee decision on 2 May 2025, the PIPC ordered SKT to notify all affected or potentially affected individuals of the data breach and implement damage prevention measures. Information exposed in the breach included sensitive data such as mobile numbers, IMSI, authentication keys, due to a malware virus on 18 servers dating back to June 2022. PIPC is conducting an independent investigation into this breach as it is a "matter of great public concerns" and is committed to making improved efforts to prevent further harm.

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

PIPC PUBLISHES GUIDE ON DATA PORTABILITY RIGHT

On 6 May 2025, the PIPC published guidance titled "Personal Information Transmission Request System Guide" which outlines detailed instructions for individuals exercising their data portability rights under the Personal Information Protection Act. The guide explains two types of requests, the sending of personal data to oneself, and the sending of data to a third party such as a personal data management agency.

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

PIPC LAUNCHES CONSULTATION ON ENFORCEMENT DECREE AMENDMENT

On 30 May 2025, the PIPC opened a consultation seeking feedback on the proposed amendments to the Enforcement Decree of the Personal Information Protection Act. The changes include establishing domestic agents for overseas businesses with a significant influence over Korean businesses and the need for overseas businesses to supervise these agents. The definition of public institution is amended to encompass local government funded organisations, meaning the public tasks basis can be used for processing personal data.

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

PIPC INVESTIGATES DATA BREACH AT DIOR AND TIFFANY & CO

On 1 June 2025, the PIPC announced that it launched an investigation into a data breach at Dior and Tiffany & Co and will investigate whether the companies implemented appropriate organisational and technical measures. The data breaches occurred due to unauthorised access of employee accounts to a SaaS-based customer management system which the PIPC will also be looking into in relation to its security practices. The PIPC recommended that organisations install two factor authentication for employee accounts and ensure the appropriate access controls are in place to protect against such threats.

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

PIPC REVIEWS META'S FACIAL RECOGNITION TOOL TO COMBAT CELEBRITY IMPERSONATION

On 28 May 2025, the PIPC concluded its Prior Adequacy Review into Meta Platforms' new celebrity impersonation protection service, which uses facial recognition

technology to detect and block scam ads featuring fake celebrity advertisements. Meta, relying on the individuals' opt-in consent, will register a celebrity into the protection service by creating and storing unique facial features of the individual. When an impersonation is suspected, Meta temporarily generates and uses facial embeddings from the flagged content for a one-time comparison only, then deletes them, adhering to strict purpose and use limitations. Meta is required to inform users about this process and provide server logs to verify compliance. The PIPC stated that the collaborative Prior Adequacy Review Mechanism helps ensure new tech developments meet evolving privacy standards and confirmed that it will monitor Meta's implementation when the service launches in Korea.

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

MALAYSIA

PDP PUBLISHES GUIDANCE ON KEY DATA PROTECTION TOPICS

On 21 May 2025, the Malaysian Personal Data Protection Authority (**PDP**) published a series of guidance documents on key data protection topics, including data breach notification requirements, and appointing a data protection officer. The guidelines aim to ensure organisations understand their reporting duties and when a data protection officer should be appointed.

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

AUSTRALIA

OFFICE OF THE INFORMATION COMMISSIONER RECORDS DATA BREACHES IN 2024

In May 2025, the Office of the Australian Information Commissioner (**OAIC**) produced statistics on the number of data breaches reported to the OAIC in 2024. Over 1,100 breaches were reported in 2024, increasing by 25% from 2023. This demonstrates growing concern over the increasing threat to personal information. 69% of the breaches were a result of a malicious and criminal attacks, such as phishing and impersonation. The OAIC called for organisations to be diligent and implement strong security and privacy measures. The OAIC's report highlighted that public sector data breaches tend to be reported much slower than those within the private sector. Given that many individuals have very limited choice but to provide their information to public authorities, they expect their data to be handled securely, the OAIC emphasised the need for quick detection and disclosure to minimise harm.

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

OAIC CALLS FOR VIEWS TO HELP SHAPE CHILDREN'S ONLINE PRIVACY CODE

On 16 May 2025, the OAIC invited the views of children, young people and parents to help shape the development of a Children's Online Privacy Code. The Code will aim to protect children's personal information on platforms such as social media and messaging apps. The code is expected to be in place by 10 December 2026. The OAIC's aim is to get key stakeholders to share their experiences to help shape a safer, more respectful online environment for the next generation. Children and parents can use the OAIC's issued age-appropriate worksheets, a discussion paper, and classroom materials to facilitate them to share their views. Feedback is open until 30 June 2025.

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

AUSTRALIAN GOVERNMENT PUBLISHES PAPER ON GEO-BLOCKING

On 19 May 2025, the Australian Government published a paper on geo-blocking, providing an overview for decision markers on the use of geo-blocking. The paper outlines the practice of blocking or denying network traffic based on the geographic assignment of IP addresses, exploring the advantages, limitations and risks of using geo-blocking.

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

NSA AND INTERNATIONAL CYBERSECURITY AGENCIES PUBLISHES AI DATA SECURITY GUIDANCE

On 22 May 2025, the Australian National Security Agency (**NSA**) in collaboration with key international cybersecurity agencies, published joint guidance on best practices for protecting data when using AI systems. The Cybersecurity Information Sheet encouraged securing of AI data supply chains through measures such as digital signatures, data provenance tracking, and use of trusted infrastructure. The guidance warns of risks of data drift and malicious data manipulation, urging organisations to implement appropriate protections throughout the lifecycle of AI models.

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

AUSTRALIAN GOVERNMENT PUBLISHES UPDATED AI MODEL CLAUSES

The Australian Government has released version 2.0 of its AI Model Clauses to help government buyers manage their vendor relationships when procuring AI-based technologies and services. The updated clauses, developed by the Digital Transformation Agency, provide a structured framework to ensure the ethical, secure, and transparent procurement of AI systems by government entities. The Model Clauses establish clear obligations between sellers and government buyers, ensuring responsible AI use and strong data protection throughout the procurement process. They also serve as a valuable reference for private-sector companies developing AI vendor agreements.

You can read the AI Model Clauses here.

GLOBAL

GLOBAL CBPR FORUM LAUNCHES CROSS-BORDER PRIVACY CERTIFICATIONS TO STRENGTHEN DATA PROTECTION

The Global Cross-Border Privacy Rules (**CBPR**) Forum officially launched the Global CBPR and Privacy Recognition for Processors (**PRP**) certifications. This came into effect 1 June 2025, offering organisations a clear way to ensure personal data protection across borders. With around 100 certified companies covering 2,000 entities, these certifications require third-party Accountability Agents to verify compliance with consistent data privacy standards, fostering trust and facilitating secure global data flows. The Forum Chair and industry leaders highlighted the certifications' role in boosting privacy, enabling trade, and encouraging innovation, while the Forum plans to address sensitive data and breach notifications.

You can read the CBPR's announcement here.