Privacy Partnership

MAY NEWSLETTER

OFCOM PUBLISHES FINAL DRAFT ONLINE SAFETY CODES TO PROTECT CHILDREN

The Online Safety Act 2023 is a groundbreaking law which seeks to protect both children and adults online, in particular by implementing strong protections to help safeguard children.

Ofcom has now released the final versions of its children's online safety codes (to be approved by parliament) and risk assessment guidance under the Online Safety Act 2023. Online service providers who are in-scope (i.e. those whose services are likely to be accessed by children) now have until 24 July 2025 to complete and record children's risk assessments.

From 25 July 2025 services must follow the measures outlined in the codes (or introduce equally effective protections) to keep child users safe from harmful content.

Dame Melanie Dawes, the Ofcom Chief Executive noted the significance, stating:

'These changes are a reset for children online. They will mean safer social media feeds with less harmful and dangerous content, protections from being contacted by strangers and effective age checks on adult content. Ofcom has been tasked with bringing about a safer generation of children online, and if companies fail to act they will face enforcement.'

INSIDE THIS ISSUE

PRIVACY PARTNERSHIP

This development highlights the importance of compliance for in-scope providers, with Ofcom emphasising the importance of child safety and enforcement risk.

The Online Safety Act (which became law in October last year) is coming into effect in phases as Ofcom releases the codes of practice and guidance.

You can read Ofcom's press release **here** and Ofcom's final draft Codes of practice **here**.

UNITED KINGDOM

UK REGULATOR ICO CALLS FOR FINANCIAL SECTOR TO IMPROVE THEIR PROCESSING OF CHILDREN DATA

On 1 April 2025, the UK Information Commissioner's Office (**ICO**) called for the financial sector to do more to improve its handling of children's data. A recent review completed by the ICO found that better data governance was needed whilst dealing with children's financial records when providing a service. Improvements include updating privacy notices as the child ages and their understanding increases, providing staff with specific training on handling children's data, the protections required and to differentiate between parental consent and the child's consent in regard to marketing.

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

ICO STRESSES THE IMPORTANCE OF RESPONSIBLE PROCESSING AS POLICE ROLL OUT FACIAL RECOGNITION

On 2 April 2025, the ICO announced its focus on ensuring the responsible use of facial recognition technology (**FRT**), specifically regarding the police's use of FRT. This includes making sure that the police only use FRT where it is necessary, proportionate and fair, given the sensitivity of personal data collected (biometric data). The UK GDPR requires extra careful handling of special category data. As the police aim to introduce officer-initiated facial recognition, it is important that they ensure they comply with data protection laws.

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

STRICTER AGE ASSURANCE BEGINS TO ROLL OUT FOLLOWING OFCOM'S ENFORCEMENT PROGRAMME

Earlier this year, Ofcom sent letters to providers outlining their legal duty under the Online Safety Act to protect children from accessing adult content. Such enforcement efforts prompted many online pornography providers to implement stricter age assurance systems to ensure their compliance. Ofcom has announced that it will continue to urge more providers to act, stressing that by 25 July 2025, all platforms hosting pornography must implement robust age verification measures. Failure to do so may result in enforcement action.

You can read Ofcom's announcement **here**, and the most recent letter to platforms **here**.

ICO FINES LAW FIRM AFTER CYBER ATTACK EXPOSES SENSITIVE DATA

On 16 April 2025, the ICO fined DPP Law Ltd £60,000 following a 2022 cyber-attack that exposed highly sensitive personal data (including legally privileged and special category information) which later appeared on the dark web. The ICO's investigation revealed that the firm failed to implement basic security measures, such as multi-factor authentication (**MFA**), on a rarely used administrator account. Hackers exploited this account to access the firm's network and steal sensitive data.

Given the nature of the information collected, the ICO emphasised the critical need for strong data protection. The regulator also found that DPP Law breached its legal obligation to report the incident within 72 hours, instead delaying notification by 43 days and failing to initially recognise it as a personal data breach.

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

AFK LETTERS CO LTD ISSUED £90,000 FINE FOR UNLAWFUL MARKETING CALLS

On 24 April 2025, the ICO fined AFK Letters £90,000 for unlawfully making 95,000 marketing calls to individuals registered with the Telephone Preference Service, violating the Privacy and Electronic Communications Regulation which requires clear, informed consent. The ICO's investigation found that AFK failed to demonstrate valid consent, did not maintain proper consent records, and used third-party consent statements that did not name AFK. The ICO also noted that AFK's privacy notice only referred to email contact and excluded mention of processing for telemarketing

purposes. Businesses should review their direct marketing strategies to ensure appropriate systems are in place to comply with data protection laws.

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

ICO RESPONSE FOLLOWING BRITISH LIBRARY CYBER ATTACK IN 2023

On 30 April 2025, the ICO issued a response to the 2023 cyberattack on the British Library. A hacker exploited the library's systems through an administrator account that lacked multi-factor authentication. The ICO praised the library's transparency, noting its published cyber incident review outlining lessons learned and improvements made. The ICO chose not to open a further investigation, citing other priorities and resource constraints. Instead, it committed to providing guidance to the library, emphasising the importance of robust security measures such as MFA.

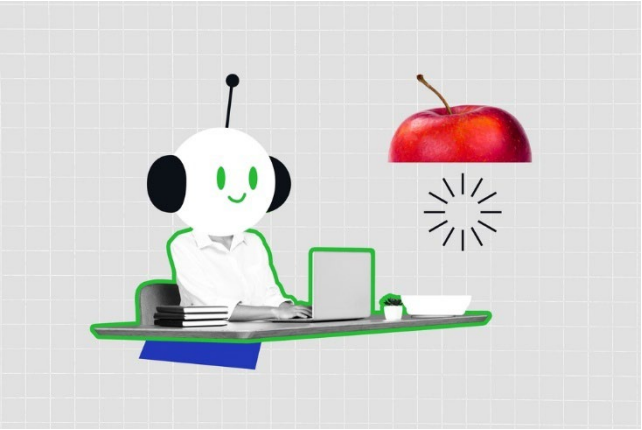
You can read the ICO's announcement **here**.

NCSC RELEASES PAPER ON ADVANCED CRYPTOGRAPHY

On 28 April 2025, the National Cyber Security Centre (**NCSC**) published a paper on "advanced cryptography" to help organisations decide when to use these technologies to protect the data they hold. Advanced cryptography refers to methods that go beyond standard encryption, offering stronger privacy and security. Techniques such as homomorphic encryption, secure multi-party computation, and zero-knowledge proofs allow organisations to process personal data without decrypting it. While these tools offer privacy advantages, the NCSC noted that the technology remains in early development stages and can suffer from slower response times, limiting practicality. The NCSC aims to guide organisations in assessing when to apply advanced cryptographic methods.

You can read the NCSC's paper **here**.

UK AI SECURITY INSTITUTE PUBLISHES PAPER ON AI AGENTS



On 11 April 2025, the UK AI Security Institute (**AISI**) published a paper on control measures for AI agents following the increase in Large Language Models (**LLMs**) becoming more autonomous. The paper explores different AI control strategies to mitigate risks imposed by AI agents and how organisations can scale such techniques to manage LLMs.

You can read the AISI's announcement here.

OFCOM ANNOUNCES ONLINE INFORMATION ADVISORY COMMITTEE

On 28 April 2025, Ofcom announced the establishment of the Online Information Advisory Committee, as required under the UK Online Safety Act. The Committee will advise on issues related to misinformation and disinformation. Its first meeting is scheduled for 16 May 2025, with five newly appointed members set to serve three-year terms. Ofcom emphasised its role in ensuring that platforms address harmful and illegal content by maintaining effective safety systems.

You can read Ofcom's announcement here.

EUROPEAN UNION

EDPB PRODUCES GUIDELINES ON PROCESSING PERSONAL DATA THROUGH BLOCKCHAINS

On 14 April 2025, the European Data Protection Board (**EDPB**) announced that it adopted guidelines during its April plenary to help organisations using blockchain technologies comply with the GDPR. The EDPB defines a blockchain as "a distributed digital ledger system that can confirm transactions and establish who owned a digital asset." The guidelines emphasise early implementation of data protection measures, clarify stakeholder roles in blockchain-related processing, and recommend that

organisations conduct a Data Protection Impact Assessment. The EDPB opened the guidelines for public consultation until 9 June 2025 and reaffirmed its commitment to working with the AI Office to align data protection rules with the AI Act.

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

EDPB ANNOUNCES EXTERNAL REPORT ON PRIVACY RISKS AND MITIGATIONS IN LLMs

On 10 April 2025, the EDPB's Support Pool of Experts Programme published a report titled "*AI Privacy Risks & Mitigations Large Language Models (LLMs)*". The report, conducted by an external expert, includes a detailed risk management methodology for LLMs to help identify and mitigate privacy risks. The report was requested by the Croatian Data Protection Authority, and helps to provide Data Protection Authorities an detailed understanding of LLMs, their risk and the data protection implications involved. The report includes use cases from real world scenarios such as chatbots, student support tools, and AI travel assistants.

You can read the EDPB's post **here**, and the report **here**.

COMMISSION SEEKS INPUT INTO SHAPING RULES FOR GENERAL PURPOSE AI MODELS

On 22 April 2025, the European Commission launched a consultation inviting stakeholders to help shape guidelines for general-purpose AI (**GPAI**) models. These non-binding guidelines aim to clarify key concepts, including what qualifies as a GPAI model, who is considered a provider, and what constitutes placing such models on the market. They will also outline the role of the AI Office in supporting compliance and explain how signing the Code of Practice can help reduce administrative burdens for providers. The consultation is open until 22 May.

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

APPLE AND META FINED BY EUROPEAN COMMISSION FOR BREACHING DIGITAL MARKETS ACT

On 23 April 2025, the European Commission fined Apple €500 million and Meta €200 million for failing to comply with the Digital Markets Act (**DMA**). The Commission found that Apple violated the anti-steering rule by preventing app developers from informing users about alternative ways to access services or cheaper offers outside the Apple App Store. The Commission ordered Apple to remove these restrictions, noting that the

company failed to justify their necessity or proportionality, which in turn restricted user choice.

The Commission also fined Meta for implementing a "consent or pay" model that did not offer users a genuinely equal alternative when declining personalised ads. In 2023, Meta presented EU users with a choice - accept personalised tracking or pay for an ad-free version. The Commission concluded that this model did not meet DMA standards, as it lacked a true opt-out option and did not offer a less data-intensive alternative.

The Commission noted that since November 2024, Meta introduced a new advertising model, which it is currently reviewing. Both Apple and Meta have 60 days to respond.

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

BEUC SENDS LETTER TO COMMISSION OPPOSING THE REVISITING OF THE GDPR

On 24 April 2025, the European Consumer Organisation (**BEUC**) sent a letter addressed to the European Commission urging them not to reopen the General Data Protection Regulation (**GDPR**) and rather focus on enforcing the GDPR to ensure consumers are protected. This follows the Commission's proposal to slightly modify the GDPR, such as exempting SMEs or even larger "small mid-cap" companies from certain obligations e.g. record keeping obligations. The BEUC raised concerns that such changes could weaken data protection and introduce significant legal uncertainty.

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

EDPB PUBLISHES ITS 2024 ANNUAL REPORT ON DATA PROTECTION MILESTONES

On 23 April 2025, the EDPB published its 2024 annual report discussing key milestones in the data protection sector. This includes the adoption of 2024-27 strategy focused on modernising data protection across the EU and addressing cross-regulatory challenges. The EDPB highlighted key achievements such as the publishing of several consistency opinions, guidance on AI, facial recognition, and "Consent or Pay" models. The EDPB developed new digital laws like the Digital Markets Act, Digital Services Act, and AI Act, building on the GDPR and through active cross-regulatory cooperation.

You can read the EDPB's announcement here.

AUSTRIA

DSB BANS VIDEO SURVEILLANCE BY PARKING MANAGEMENT COMPANY

On 16 April 2025, the Austrian Data Protection Authority (**DSB**) announced that it concluded its review into the use of video surveillance practices by a parking management company following multiple complaints from the public. The DSB's review led to the company receiving an immediate ban on the use of video surveillance for monitoring parking spaces within Austria. It was found to have violated the GDPR.

You can read the DSB's announcement here and the decision here.

NOYB FILES COMPLAINT AGAINST UBISOFT TO AUSTRIAN DSB

On 24 April 2025, noyb announced that it filed a complaint with the Austrian DSB against French company Ubisoft for allegedly processing personal data without a lawful basis. Ubisoft requires players to connect to the internet and log in (even for single-player games). This allowed the company to track gameplay sessions without user consent. One complainant found that within 10 minutes of using the platform, their data was shared with third parties 150 times. Since Ubisoft did not obtain consent, noyb is asking the DSB to declare the processing unlawful, order deletion of the data, and stop any further tracking without a valid legal basis.

You can read noyb's announcement here.

CROATIA

CROATIAN INFORMATION SYSTEMS SECURITY BUREAU PUBLISHES PROPOSAL ON CYBERSECURITY SELF ASSESSMENTS

The Croatian Institute for Information Systems Security (**ZSIS**) published its "Draft Proposal of the Guidelines for the Implementation of Cybersecurity Self-Assessment" as part of Article 57 of the Information Systems Security Act. The Guidelines alongside its three annexes (self-assessment calculator, risk management evaluation framework, and catalogue of controls) are open for public consultation until 15 May 2025.

You can read the ZSIS's announcement here and the guidelines here. (Only available in Croatian)

DENMARK

DATATILSYNET ANNOUNCED ACTION TO ENSURING RIGHT TO ERASURE

On 25 April 2025, Denmark's Data Protection Authority, Datatilsynet, announced that it will investigate online casino companies as part of the EDPB's 2025 coordinated enforcement action. The inspections will assess how these companies handle data deletion requests and identify any challenges in complying with the right to erasure. Datatilsynet will use the findings to inform its national report and contribute to the EDPB's broader assessment.

You can read the Datatilsynet's announcement here.

ESTONIA

ESTONIAN AKI PUBLISHES DATA SECURITY RECOMMENDATIONS FOR E-COMMERCE BUSINESSES

On 29 April 2025, the Estonian Data Protection Inspectorate (**AKI**) published a guide to help e-commerce businesses (e-shops) strengthen customer data security and manage cyber risks. Taking into account the GDPR and the Electronic Communication Act, the guidance offers clear recommendations on security measures and includes advice on incident response and staff training to help businesses reduce the risk of data breaches.

You can read the AKI's announcement here and the guidance here.

FRANCE

FRENCH REGULATOR CNIL ISSUES RECOMMENDATIONS ON MULTI-FACTOR AUTHENTICATION

On 1 April 2025, the French Data Protection Authority (**CNIL**) published its recommendations on multi-factor authentication (**MFA**) solutions to improve data protection and cybersecurity measures to comply with GDPR principles. This guidance is aimed at helping users and providers implement MFA in a way that ensures privacy by design, especially when personal data is involved.

You can read the CNIL's announcement here, and the recommendation here (Only available in French).

CNIL REVEALS ITS DATA PROTECTION STRATEGY FOR 2025-28

On 14 April 2025, the CNIL published its European and international strategy for 2025–2028, aiming to strengthen its role in shaping global data protection. The strategy focuses on three key areas - enhancing European cooperation to adapt personal data protection to new digital regulations, promoting high international data protection standards while supporting innovation and data flows and reinforcing CNIL's global influence by advocating a balanced model of privacy.

You can read the CNIL's announcement here.

CNIL CALLS FOR VIEWS ON DRAFT RECOMMENDATION FOR MULTI DEVICE CONSENT COLLECTION

On 24 April 2025, the CNIL invited stakeholders to provide feedback on its draft recommendation for multi-device consent collection. The aim is to support GDPR compliant consent practices in response to rising use of connected devices and the need for consistent consent across platforms. The draft targets "logged universes," where users are authenticated to an account and give consent on one device, which then applies to all others linked to the same account. The consultation runs until 5 June 2025.

You can read the CNIL's announcement here.

CNIL REINFORCES THE NEED FOR SECURITY FOLLOWING INCREASE IN DATA BREACHES

On 30 April 2025, the CNIL published recommendations on how organisations can help strengthen their security to ensure data protection, following a high number of reported data breaches in 2024. The CNIL reminded organisations that under the GDPR they are required to have an "appropriate level of security" and recommended the adoption of multi-factor authentication as an essential protection for databases. Key recommendations also included strict logging and data flow monitoring, implementing role-based access control, conducting regular user awareness training, and including clauses within agreements around the need to adhere to security obligations.

You can read the CNIL's announcement here.

GERMANY

HAMBURG DPA ADVISES USERS TO OBJECT TO META'S USE OF PERSONAL DATA TO TRAIN AI MODEL

On 15 April 2025, Hamburg's Data Protection Authority (**DPA**) announced that Meta will begin using personal data from European users of Facebook and Instagram to train its AI models starting at the end of May 2025. This data will include any posts and photos users have made public. The Hamburg DPA reminds users that if they do not want their personal data to be used, they must opt out via Meta's official channels before the end of May. After this deadline, Meta may use the data, and it cannot be removed from the AI models, as AI systems cannot unlearn information once trained - making the decision irreversible.

You can read the DPA's announcement here.

HAMBURG DPA PRODUCES Q&A ON THIRD PARTY TRACKING TOOLS

On 24 April 2025, the Hamburg DPA produced a Q&A on third party tracking tools on websites as part of its ongoing monitoring of organisation's website compliance with data protection laws. The Q&A is aimed at helping organisations understand their responsibilities in ensuring transparency and lawful collection of data.

You can read the DPA's announcement here.

HAMBURG DPA PRODUCES GUIDE ON EU DATA ACT

On 29 April 2025, the Hamburg DPA produced guidance on the EU Data Act which is set to enter into force 12 September 2025. This will require that manufacturers of internet-enabled devices grant third parties' access to the data their products generate, including from vehicles, appliances, and industrial machines.

You can read the DPA's announcement here.

GREECE

GREEK AUTHORITY PROVIDES TRAINING AND MATERIALS FOR AI USE

On 8 April 2025, the Greek Data Protection Authority (**DPA**) launched specialised training programs to help professionals navigate the intersection of AI and data protection law. External experts, under the guidance of the EDPB and DPA scientists, developed the content to upskill Data Protection Officers (**DPOs**), privacy professionals, and ICT specialists with key legal, ethical, and technical knowledge. The initiative covers topics such as the European AI Regulation, principles of fairness and transparency in AI, and best practices for secure implementation.

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

DPA REINFORCES THE NEED FOR ORGANISATIONS TO IMPLEMENT THE DATA MINIMISATION PRINCIPLE

On 16 April 2025, the Greek Data Protection Authority (**DPA**) announced that it reviewed a case involving the publication of debtor's personal data on the electronic auction platform E.S.P.L.S. To comply with GDPR principles of data minimisation and data protection by design and by default, the Notary Association of the Courts of Appeal of Athens, Piraeus, Aegean, and Dodecanese developed an application to hide debtor data once the legal basis for its publication ends. Authorities implemented this nationwide on 10 April 2025. The DPA reiterated that data controllers must design processing activities to include only necessary data and should always consider less intrusive technical measures - such as pseudonymisation where possible, in line with the principle of proportionality.

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

IRELAND

IRISH DATA PROTECTION AUTHORITY ANNOUNCES INQUIRY INTO GROK USE OF PUBLIC POST OF X

On 11 April 2025, the Irish Data Protection Commission (**DPC**) begun an inquiry into whether the platform X is lawfully using personal data from publicly accessible posts by EU/EEA users to train its AI model, Grok. The DPC's investigation aims to assess X's compliance with the requirements of the GDPR with a particular focus on the lawfulness and transparency of the data processing. Grok, a group of large language models, includes powering an AI chatbot on the X platform and was trained using various data sources, including posts controlled by X Internet Unlimited Company.

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

DPC FINES TIKTOK €530 MILLION FOR UNLAWFUL DATA TRANSFERS TO CHINA

On 2 May 2025, the Irish Data Protection Commission (**DPC**) announced that it imposed a €530 million fine against TikTok for its unlawful transfer of European user's personal data to China, and for failing to inform users of this transfer. TikTok was found to have violated Article 46(1) of the GDPR by failing to ensure that Chinese laws provided adequate data protections as equivalent to EU standards, and for not by properly assessing and guaranteeing such protections. The DPC's inquiry also revealed that TikTok's privacy statements were non-compliant, as they failed to name the third countries such as China in which data was being transferred. Nor did they provide clarity to users of the nature of data transfers. Alongside the fine, TikTok has six months to bring its data processing into compliance or face the suspension of its transfers of data to China.

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

ITALY

ITALIAN REGULATOR, GARANTE, PUBLISHES GUIDANCE TO PROTECT AGAINST SMISHING

On 2 April 2025, the Italian Data Protection Authority (**Garante**) published guidance on smishing - a form of phishing via SMS and messaging apps used by scammers to steal personal and financial data. These fraudulent messages often create a false sense of urgency, urging victims to click malicious links, download infected attachments, or disclose sensitive information such as PINs, passwords, or banking credentials. The Garante reiterated that official institutions and banks never request such information through SMS or messaging platforms. It also warned users to avoid clicking links or opening attachments from unknown or suspicious senders, especially those using urgent or threatening language.

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

GARANTE INVESTIGATES LUSHA DATA COLLECTION PRACTICES

On 8 April 2025, the Garante announced its decision to investigate Lusha Systems Inc., a U.S.-based company selling contact information such as email addresses and phone numbers. The service is accessible to Italian citizens, and confirmed cases show that data on Italian residents appear in Lusha's database. Reports have also alleged that the company conducted unsolicited marketing calls. The Garante has requested that Lusha clarify its data sources, whether it obtains consent for commercial use, and how it processes data on individuals in Italy. Lusha has 20 days to respond.

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

GARANTE AND CARABINIERI SIGN MOU TO TACKLE CYBER RISKS

On 18 April 2025, the Garante and the Italian Carabinieri (police force) signed a Memorandum of Understanding to strengthen collaboration on digital safety, personal data protection, and combating cyber threats such as cyberbullying and revenge porn. The agreement focuses on training initiatives, public awareness campaigns, and other operational activities. The Carabinieri will support these efforts by helping to distribute educational materials and promote awareness.

You can read the Garante's announcement here.

LATVIA

DVI PROVIDES GUIDANCE ON SCHOOL OBLIGATIONS IN REGARDING TO VIDEO SURVEILLANCE FOOTAGE

In April 2025, Latvia's Data Protection Authority (**DVI**) published guidance to help schools understand their responsibilities regarding video surveillance footage. As schools increase their use of surveillance systems to ensure safety and protection, many parents have requested access to footage to observe their child's activities or resolve conflicts. While the GDPR permits parents to access personal data about their child, the DVI emphasises the limits and responsibilities schools must observe. The guidance explains how educational institutions can responsibly balance individual privacy rights with legitimate parental requests.

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

DVI GUIDANCE FOR POSTING ON SOCIAL MEDIA

The DVI published guidance to clarify to social media content creators that any photos and videos capturing other people for commercial purposes is to be regarded as personal data, and the GDPR is applicable. As a result, creators must follow the necessary legal requirements, including informing individuals about the processing of their data, the purpose, and the legal basis for doing so. The DVI advises against posting content that depicts individuals negatively or invades their privacy. If someone exercises their right to erasure, the DVI encourages creators to respect the request by either anonymising the data or deleting the content entirely.

You can read the DVI's announcement here.

LITHUANIA

VDAI REMINDS USERS OF OPT OUT RIGHT FOLLOWING META'S USE OF PERSONAL DATA TO TRAIN AI

On 18 April 2025, the Lithuanian Data Protection Inspectorate (**VDAI**) alerted users of Meta platforms of the company's decision to start using public posts, photos and comments posted by adult European users to train its AI model at the end of May 2025.

Should users not wish to be included in this training, they are able to opt out via the applicable platform's help centre.

You can read the VDAI's announcement here.

VDAI PUBLISHES GUIDANCE ON DATA PROTECTION OFFICERS

On 16 April 2025, the VDAI published new guidance for organisations to help understand the role and requirements of a data protection officer (**DPO**) e.g. by explaining when a DPO is required, what qualifications they should have and how to avoid conflicts of interest. The guidance also includes the implementation of the DPO's tasks in practice to ensure independency.

You can read the VDAI's announcement here.

VDAI SHARES SUMMARY OF WEBSITE COOKIES FINDINGS

On 7 April 2025 the VDAI produced a summary of several websites' use of cookies in order to share good practices with the public for ensuring cookie compliance. This followed the VDAI's investigation in 2024, which looked at how websites use cookies and how they can improve their practices.

You can read the VDAI's announcement here.

LUXEMBOURG

CNPD PRODUCES GUIDELINES FOR TRANSFERRING PERSONAL DATA OVERSEAS

On 18 April 2025, the National Commission for Data Protection for Luxembourg (**CNPD**) published guidelines for organisations to help clarify what constitutes a transfer of personal data to a third country and outlines the conditions for transferring. The CNPD's guidelines explain that third countries with an adequacy decision from the European Commission can benefit from data transfers as they are deemed to offer an adequate level of data protection. Where a country is not listed within an adequacy decision, the guidelines provide other tools and information such as the EU standard contractual clauses to help guide organisations in complying with the GDPR.

You can read the CNPD's announcement here.

MALTA

MALTESE IDPC PRODUCES FAQS ON RETAINING EMPLOYEE EMAIL ACCOUNTS AFTER DEPARTURE

On 11 April 2025, Malta's Information and Data Protection Commissioner (**IDPC**) published FAQs to help employers understand and manage their ex-employees' email accounts, to ensure compliance with the GDPR. Employers (although they may have a legitimate interest in retaining the email address) must also respect the privacy and data protection rights of individuals and others concerned. The FAQs aim to promote a structured, transparent approach -covering best practices for auto-forwarding, out-of-office replies, and handling personal correspondence.

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

NETHERLANDS

DUTCH AUTHORITY AP FINDINGS FOLLOWING INVESTIGATION INTO COOKIE BANNERS

On 8 April 2025, the Dutch Data Protection Authority (**AP**) concluded its investigation into five websites and found all of them in violation of cookie consent rules. The websites hid reject buttons or used pre-ticked boxes, leading to cookie tracking without users' clear knowledge or consent. All organisations involved have since implemented proper consent mechanisms to comply with the law. The AP confirmed plans to investigate more websites for similar issues.

On 15 April 2025, the AP sent letters to 50 organisations warning them to improve practices or risk the AP conducting an investigation within 3 months. In cases of serious non-compliance, the AP may issue fines.

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

AP TO SUPPORT DUTCH ORGANISATIONS AMIDST STRUGGLE WITH ALGORITHM USE

The AP announced that (following a recent survey) many Dutch organisations reported lacking resources, awareness, and control over how algorithms process personal data. Most organisations did not know whether or how they use algorithms, often

outsourcing to external suppliers without fully understanding the risks. To help, the AP plans to provide practical tools, including checklists and guidance on the importance of human oversight. Additionally, with the EU AI Act now in force, organisations must implement AI literacy, and the AP has issued guidance to help organisations.

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

POLAND

PUBLIC BROADCASTERS ARE REMINDED OF THE NEED TO PROTECT INDIVIDUAL'S PERSONAL DATA

On 9 April 2025, the Polish Personal Data Protection Office (**UODO**) reminded all public broadcasters to protect the personal data of individuals featured in their stories. The reminder followed a case in which Polish Radio Szczecin disclosed the personal data of a child who later died by suicide. UODO fined the station for failing to safeguard this data - an omission that can endanger lives. While journalistic activities may be exempt from certain GDPR provisions, UODO emphasised that public broadcasters must still have policies and safeguards in place, including consent procedures, anonymisation measures, and proper oversight.

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

FUNERAL HOME FINED FOR MISHANDLING OF PERSONAL DATA

On 15 April 2025, the UODO fined a funeral home PLN 33,000 for its mishandling of the personal data it collected, including for failure to secure the personal data contained in burial documents. It found that boxes of these documents, of a sensitive nature, were found abandoned on the side of the road after falling from an unsecure vehicle during transit. The home failed to report this to the UODO.

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

UODO WARNS OF PRIVACY IMPLICATIONS REGARDING BODY CAMERA USE BY PARAMEDICS

On 23 April 2025, the UODO made clear that audio-visual body cameras on paramedics should be a last resort and only used when less invasive safety measures are inadequate. Any use of body cameras must comply with individuals' rights to privacy and data protection. This would require a data protection impact assessment

(**DPIA**) to be conducted to ensure necessity, proportionality, and legal justification under the GDPR and Polish law, given that the use of such monitoring could significantly impact both patients' and paramedics' rights.

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

ROMANIA

ROMANIAN AUTHORITY FINES BINBOX GLOBAL FOR SECURITY FAILURES

On 2 April 2025, Romania's National Supervisory Authority for Personal Data Processing (**ANSPDCP**) imposed a €3,000 fine on Binbox Global Services S.R.L. for failing to implement adequate security measures, in breach of Article 32 of the GDPR. The ANSPDCP launched its investigation after a cyber-attack encrypted the company's IT systems, resulting in unauthorised access to and disclosure of personal data. The authority found that Binbox had failed to apply sufficient technical and organisational measures to protect personal data and secure its IT systems.

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

ANSPDCP FINES LENSA.RO FOR UNLAWFUL MARKETING AND FAILURE TO MEET GDPR RIGHTS REQUESTS

On 10 April 2025, the ANSPDCP fined Tensa Art Design S.A., owner of Lensa.ro, €15,000 for processing a user's personal data (including their phone number) for direct marketing without obtaining consent. The authority also found that the company failed to properly handle the user's GDPR access and deletion requests. In addition, the ANSPDCP imposed corrective measures, requiring the company to improve staff training, collect valid consent, and establish proper procedures for responding to data subject rights.

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

TRAVEL PLANNER SRL FINED FOR FAILING TO NOTIFY BREACH AND MISHANDLING OF ACCESS REQUESTS

In April 2025, the ANSPDCP imposed a €6,000 fine (and a warning) against SC Travel Planner SRL for publishing the personal data of tourists on Facebook during a raffle.

The company had failed to implement sufficient technical and organisational measures which led to the unauthorised disclosure of personal data. The company did not report this breach to the ANSPDCP. The ANSPDCP also found that the company did not respond properly to access requests.

You can read the ANSPDCP's announcement here.

SLOVENIA

SLOVENIA AUTHORITY IP TO PROMOTE CHILDREN ONLINE SAFETY

On 18 April 2025, the Slovenian Information Commissioner (**IP**) announced the launch of PrivacyPro Project - aimed at raising awareness of children and minors about data protection. The IP has created workshops, manuals and guidance for schools to help improve data protection understanding and knowledge sharing between students, teachers and stakeholders. The IP aims to raise awareness on the importance of children's online safety.

You can read the IP's announcement here.

SPAIN

CATALAN DPA NEW RESPONSIBILITES UNDER EU AI ACT

On 11 April 2025, the Catalan Data Protection Authority (**APDCAT**) announced new duties under the EU AI Act, including oversight of high-risk AI systems and protection of fundamental rights. APDCAT will handle notifications on remote biometric identification, submit annual reports to the Commission, and join controlled AI testing environments. It will also access key documentation to ensure compliance and promote public awareness on responsible AI use.

You can read the APDCAT's announcement here.

SWEDEN

SWEDISH AUTHORITY, IMY, INVESTIGATES SEARCH DATABASES AND THE PUBLISHING OF CRIMINAL OFFENCE DATA

On 2 April 2025, the Swedish Data Protection Authority (**IMY**) launched investigations into two search service databases, Lexbase.se and Krimfup.se, for publishing criminal records. IMY received numerous complaints, and a recent Supreme Court ruling found that large-scale publication of such records is incompatible with EU data protection

laws. IMY's investigations aim to determine whether these services are violating the GDPR.

You can read the IMY's announcement here.

IMY INVESTIGATES SPORTADMIN FOLLOWING DATA BREACH

On 15 April 2025, the IMY begun its investigation into Sportadmin following a reported personal data breach in its association management service. The IMY's investigation was initiated because of over 1,650 breach reports from sports clubs, indicating Sportadmin acts as a personal data processor for their organisation. IMY will assess whether the company implemented appropriate technical and organisational safeguards to determine its compliance with GDPR.

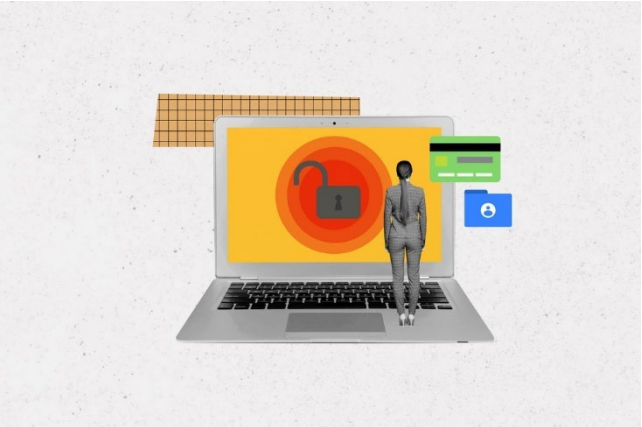
You can read the IMY's announcement here.

HOSPITAL BOARD REPRIMANDED BY IMY FOR EMAIL DATA BREACH

On 25 April 2025, the IMY reprimanded Uppsala's Hospital Board for failing to implement adequate security measures when handling sensitive health data via email. Despite rules prohibiting the unencrypted transmission of sensitive data, the IMY found prolonged misuse and inadequate oversight of email practices among approximately 6,400 healthcare staff. As a result, the IMY concluded that the Board violated the GDPR by failing to implement effective technical and organisational measures to prevent unlawful data processing.

You can read the IMY's announcement here.

IMY FINES OMBUDSMAN FOR INSUFFICIENT SECURITY MEASURES RESULTING IN DATA BREACH



On 29 April 2025, the Swedish IMY announced that it imposed a SEK 100,000 fine on the Equality Ombudsman for failing to implement adequate security measures on its online complaint form, which led to a data breach. The Ombudsman attempted to hide data from web

analytics, but the function failed, and the issue went unnoticed until after the breach. As a result, the personal data (and possibly sensitive information) of approximately 500 discrimination complaints was disclosed to an external data processor hired to conduct analysis. After discovering the breach, the Ombudsman shut down the web form immediately to prevent further exposure.

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

3 COMPANIES REPRIMANDED BY IMY FOLLOWING NON-COMPLIANT COOKIE BANNERS

On 30 April 2025, IMY reprimanded three companies following complaints about their cookie banners. One company failed to inform users of their right to withdraw consent and did not provide an option to do so. Another company used a misleading banner design that made it difficult for users to give freely informed consent. The third company relied on legitimate interest as a legal basis for processing but lacked proper justification.

IMY reminds organisations that cookie banners must enable users to make informed choices and include clear options to withdraw consent.

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

CANADA

QUEBEC COMMISSION NOTIFIES INDIVIDUALS OF THEIR RIGHT TO DELETE FOLLOWING 23ANDME BANKRUPTCY

On 17 April 2025, Quebec's Privacy Commission (**CAI**) reminded 23andMe customers of their rights to protect personal data following the company's bankruptcy filing. Although 23andMe stated that its privacy policy will continue to apply to personal data - even if the information is transferred during bankruptcy proceedings - the Commission urged citizens to exercise their privacy rights due to uncertainty over future data use. Customers are encouraged to review their privacy settings and consider exercising their right to deletion to retain control over their data.

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

UNITED STATES OF AMERICA

TEXAS ATTORNEY GENERAL PUSHES FOR CITIZENS PROTECTION FOLLOWING 23ANDME FILING FOR BANKRUPTCY

On 21 April 2025, the Texas Attorney General (**AG**) filed a motion to appoint a Consumer Privacy Ombudsman to help protect Texans' sensitive genetic and personal data following 23andMe's bankruptcy filing. The AG raised concerns that the company may sell assets, including personal and genetic data. The AG urged Texans to exercise their rights to data deletion under state law and encouraged them to file complaints if they encounter difficulties. The case highlights the complex intersection between bankruptcy proceedings and data protection implications.

You can read the Attorney General's announcement **here**.

FLORIDA ATTORNEY GENERAL FILES ACTION AGAINST SNAPCHAT

On 22 April 2025, Florida's Attorney General filed legal action against Snap Inc., the company behind Snapchat, for violating the Florida Deceptive and Unfair Trade Practices Act. The AG alleges that Snapchat uses addictive design features (such as notifications, snap streaks, and autoplay videos) to encourage excessive use. The AG also accuses Snap of misleading parents by promoting the platform as safe for children, despite its exposure to harmful content. Additionally, it claims Snap fails to obtain parental consent for users aged 14–15, violating Florida law.

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

FTC AMENDMENTS TO COPPA PUBLISHED TO FEDERAL REGISTER

On 22 April 2025, updated amendments to the Children's Online Privacy Protection Rule (**COPPA**) made by the Federal Trade Commission (**FTC**) were published within the Federal Register. This is aimed at ensuring proper safeguards are in place to restrict the processing of children under 13. The COPPA Rule will be effective from 23 June 2025, with organisations required to comply by 22 April 2026.

You can read the Rule here.

FLORIDA AIMS TO PROMOTE ONLINE SAFETY FOR CHILDREN AND ISSUES SUBPOENA AGAINST ROBLOX

Florida's Attorney General announced the issuance of a subpoena to Roblox, the gaming platform, requesting information about its marketing to children, age-verification processes, and chat room moderation. The action follows reports indicating that children and minors have been exposed to harmful content and contacted by online predators. Statistics show that approximately 40% of Roblox users are under the age of 13.

You can read the AG's announcement here.

TEXAS AI REGULATION PROGRESSES

On 23 April 2025, the Texas House passed House Bill 149 "the Texas Responsible Artificial Intelligence Governance Act" which aims to promote the development of AI whilst protecting the public from harm by providing regulatory clarity, establishing a sandbox program, and implementing legal safeguards. The Bill is now set to move to Texas Senate.

You can read the announcement here, the Bill here, and to track progress here.

COURT FINDS GOOGLE IN VIOLATION OF DIGITAL ADVERTISING

On 17 April 2025, the New York Attorney General announced that the U.S. District Court ruled in favour of the AG and 16 other state attorneys general in their antitrust case against Google. The court found that Google used its dominance in digital advertising to impose anticompetitive policies, unlawfully tied its ad services, and made it harder for websites to earn revenue - extracting excessive profits and undermining fair competition. The 2023 lawsuit was led by New York and joined by the Department of Justice and 17 states. A second trial phase will determine remedies to restore competition in the online advertising industry.

You can read the AG's announcement here.

ENERGY AND COMMERCE COMMITTEE ANNOUNCES INVESTIGATION INTO DEEPSEEK

On 24 April 2025, the U.S Energy and Commerce Committee **(E&C**) announced an investigation into DeepSeek following concerns over the company's transfers of data to China. The E&C have requested further information from DeepSeek regarding its data practices (including types of personal data collected and its sources used to train their AI model), the security controls in place regarding AI model development, and ties to the Chinese government.

You can read the E&C's announcement **here**, and the letter **here**.

NEW JERSEY AG SUES DISCORD FOR MISLEADING PRACTICES HARMING CHILDREN

On 17 April 2025, the New Jersey AG announced legal action against Discord for its use of deceptive practices to mislead parents regarding the app's ability to protect children from online predators - violating state consumer protection laws. Although Discord claims that safety features like "Safe Direct Messaging," help protect minors, its default settings allow for unsupervised and unmoderated interactions, which expose children to explicit content and grooming.

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

CALIFORNIA PRIVACY PROTECTION AGENCY SIGNS DECLARATION WITH UK ICO

On 29 April 2025, the California Privacy Protection Agency (**CPPA**) and the UK ICO signed a declaration of cooperation to help improve privacy and data protection collaboration through initiatives such as joint research, knowledge and best practices sharing, staff engagement meetings and developing appropriate methods for cooperation.

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

ARGENTINA

DATA PROTECTION AUTHORITY AAIP INITIATES TRAINING FOR ACCESS TO INFORMATION FOR PUBLIC AUTHORITIES

On 7 April 2025, the Argentinean Data Protection Authority (**AAIP**) launched a series of detailed training initiatives to help public sector employees improve their skills when responding to access to information requests. A virtual course is now available.

You can read the AAIP's announcement here.

BRAZIL

BRAZILIAN ANPD ATTENDS GLOBAL AGE ASSURANCE SUMMIT

On 11 April 2025, the National Data Protection Authority of Brazil (**ANPD**) announced its commitment to ensuring online safety for children and young people. This follows the ANPD attending the Global Age Assurance Standards Summit 2025 in Amsterdam which gathered global regulators and experts to discuss international standards for age verification in digital environments. The ANPD shared its approach to tackling online safety.

You can read the ANPD's announcement here.

ANPD FINDINGS AFTER INVESTIGATIONS INTO 20 COMPANIES TO STRENGTHEN DATA SUBJECT RIGHTS COMPLIANCE

On 25 April 2025, the ANPD announced that after its investigations into companies processing significant large volumes of personal data in November 2024, such companies are now meeting the General Data Protection Law requirements. The investigation focused on their lack of a designated data protection officer or their failure to meet data subject requests. The companies will be monitored for 6 months to ensure compliance with their obligations.

You can read the ANPD's announcement here.

CHINA

CHINESE CYBERSPACE ADMINISTRATION PUBLISHES Q&A ON CROSS BORDER DATA TRANSFER POLICY

On 9 April 2025, the Cyberspace Administration of China **(CAC)** published a Q&A to help organisations improve their understanding and compliance with China's data transfer security framework, and to help share their own policies to manage data transfers. This follows an increase in organisations interacting with companies outside of China.

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

CAC TACKLES THE EXPLOITATION OF MINORS ONLINE

On 18 April 2025, the CAC and its internet information departments announced plans to crack down on the online exploitation of minors. So far, they have banned 11,000 accounts involved in harmful practices, including staged violence with weapon-like props, inappropriate role-plays of minors as adults, and content promoting wealth, offensive language, or adult behaviour. The CAC committed to prioritising children's best interests and will remove accounts that violate these standards. It also reminded families to activate "Minor Mode," which includes time limits, safe content filters, and other tools to help protect children online.

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

CAC LAUNCHES CAMPAIGN TO PREVENT ABUSE OF AI USE

On 30 April 2025, the CAC announced that it is launching a 3-month campaign to help address the misuse of AI by starting to clean up illegal AI products, such as those technologies which clone voices and faces without consent. It will also look at lax data management of AI training and security practices.

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

HONG KONG

PCPD PUBLISHES UPDATES TO GUIDE FOR CIVIL DATA PRIVACY CLAIMS

On 17 April 2025, Hong Kong's Office of the Privacy Commissioner for Personal Data (**PCPD**) published an updated leaflet outlining the legal assistance scheme available for individuals pursuing civil claims related to breaches of the Personal Data (Privacy) Ordinance. The update aims to raise public awareness of the rights and legal remedies available to those affected by data privacy violations. The PCPD also encourages individuals to consider alternative dispute resolution methods to facilitate out-of-court settlements.

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

SOUTH KOREA

PIPC FINES CLASSU INC AND KT ALPHA FOLLOWING DATA BREACH

On 10 April 2025, South Korea's Personal Information Protection Commission (**PIPC**) announced that it fined Classu Inc. and KT Alpha for violations of the Personal Information Protection Act (**PIPA**). The PIPC issued a fine of KRW 60.8 million to Classu Inc. following a data breach affecting 1.6 million users, caused by weak access controls, unencrypted personal data, and the prolonged storage of identity documents.

PIPC also fined KT Alpha KRW 11.81 million after a credential stuffing attack exposed around 98,000 accounts and compromised the personal information of 51 users. The PIPC acknowledged that KT Alpha used adequate data masking, which limited the number of accounts affected.

Both companies failed to meet breach reporting deadlines. The PIPC issued corrective orders requiring them to improve data protection and incident response measures.

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

PIPC PUBLISHED GUIDANCE ON PRIVACY POLICIES

On 21 April 2025, the PIPC updated its guidance on privacy policies to help organisations prepare for the 2025 policy evaluation system under Article 30 of the PIPA. The guidance clarifies the distinction between personal data that can be processed without consent (e.g. to fulfil a contract) and data that requires consent. It also encourages a broader approach when listing types of data collected and retention

periods if providing a full list is impractical. Policies must also include contact details for the person responsible for handling data subject rights requests.

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

PIPC UPDATES FINDINGS ON DEEPSEEK

On 24 April 2025, the PIPC announced the findings of its investigation into DeepSeek. The Commission found that DeepSeek's privacy policy violated data protection laws by failing to provide a Korean-language version, omitting contact details, and lacking information on data security and retention. The company also transferred personal data overseas without user consent and did not implement proper age verification for users under 14. In response, DeepSeek amended its privacy policy, ceased unnecessary data transfers, and introduced an opt-out mechanism for the use of public data in AI training. It also strengthened its security measures, including age checks for minors. DeepSeek must submit a corrective action report within 60 days and follow further recommendations under ongoing PIPC supervision.

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

MEET THE NEW MEMBERS OF PRIVACY PARTNERSHIP

Privacy Partnership are excited to announce three outstanding privacy professionals have joined our team. Each one brings their own expertise in ensuring data protection, and they all have a strong legal practice background.

Alice Crawford: Senior Privacy Consultant

Alice has over a decade of experience in commercial and data privacy. She has worked across legal, regulatory, and advisory roles to help organisations navigate the complexities of data protection compliance. Her experience throughout her career has given her deep expertise in global privacy laws, including GDPR, CCPA, other US State laws, and the evolving regulatory landscape surrounding AI governance.

Alice helps clients develop and implement compliance programs, manage regulatory inquiries, and mitigate data protection risks.

Jennie Sumpster: Privacy Counsel

Jennie has been working in the field of data protection and privacy since qualification in 2007, working in private practice, in-house and as a consultant with some of the world's most innovative and disruptive brands, from start-ups to multi-nationals. She is a qualified solicitor and is a Certified Information Privacy Professional (CIPP/E)

Jennie supports her clients handling of day-to-day data protection compliance matters, particularly those within an employment law context including delivering specialist training, drafting policies and handling DSARs.

Jo Murphy: Senior Privacy Consultant and Chief Operating Officer

Jo has 20 years of experience as a UK qualified solicitor, both in private practice and in-house, and is a qualified privacy practitioner (CIPP/E). She has extensive experience working in international businesses in the media & entertainment sector including in video games, broadcast media, outdoor advertising and adtech.

Jo is known for bringing clarity to complex legal and privacy matters including advising on cookies and other tracking technologies, assessing lawful bases for complex data processing, analysing controller and processor roles in ambiguous business scenarios and advising on transparency issues within chains of data processing.