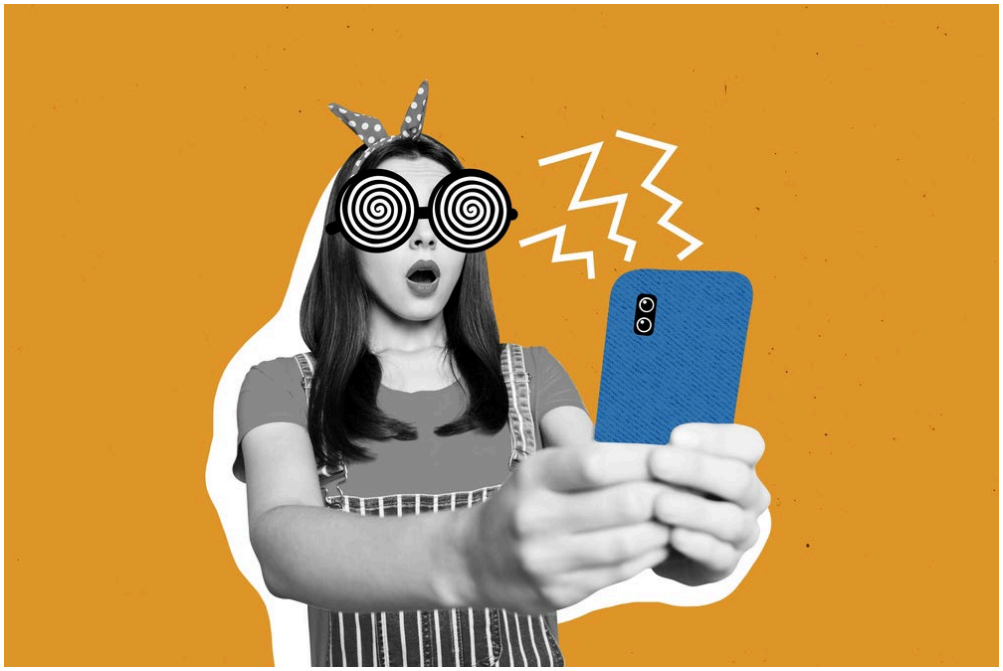
Privacy Partnership NEWSLETTER



ICO PUBLISHES "CONSENT OR PAY" GUIDANCE

On 23 January 2025, the ICO published guidance for organisations considering or implementing the "consent or pay" advertising model. The model presents users with a choice of either consenting to the use of their personal information for personalised advertising or choosing to pay a fee to access the service without this tracking enabled. The ICO's guidance aims to clarify how organisations can implement "consent or pay" models, ensuring that users are presented with clear choices and emphasising the need for users to provide their freely given and informed consent. The guidance includes important information regarding how consent or pay mechanisms can comply with data protection laws, subject to their design. It is vital that businesses using or considering "consent or pay" carefully review the ICO's guidance. The ICO (as part of its 2025 strategy) aims to engage with Consent Management Platforms who often provide organisations with tools to manage their online consent.

You can read the ICO's guidance here.

INSIDE THIS ISSUE

PRIVACY PARTNERSHIP

UNITED KINGDOM

ICO ENCOURAGES ENTREPRENEURS TO PRIORITISE DATA PROTECTION

On 2 January 2025, the Information Commissioner's Office (**ICO**) urged entrepreneurs and new businesses to implement data protection measures early into their operations, to ensure compliance with data protection regulations. The ICO has produced a beginner's guide to data protection offering eight steps to get started, as well as many other tools such as the privacy notice generator and how to videos.

You can read the ICO's announcement here.

DUA BILL COMPLETES REPORT STAGE IN HOUSE OF LORDS

On 28 January 2025, the House of Lords concluded its further checks on the Data (Use and Access) Bill (**DUA Bill**) in the Report Stage. Proposed amendments included to strengthen the Information Commissioner's independence, safeguard the processing of children's personal data through establishing Codes of Practices for Children, including in education and AI, and to address the non-consensual sexually explicit image creation. The latest list of amendments put forward in the Report Stage will be discussed during the 3rd reading in the House of Lords on 5 February 2025.

You can read the Government's announcement here.

UK GOVERNMENT ADOPTS SOFT OPT-IN AMENDMENT FOR CHARITY FUNDRAISING

The UK Government have adopted an amendment proposed by the Data & Marketing Association (**DMA**) to extend "soft opt-in" to charity fundraising. The Data Use (and Access) Bill introduces the amendment that charities could be allowed to send or arrange the sending of marketing communications if the marketing is solely used to further the charity's charitable purposes, the recipient's contact details were obtained where they have expressed an interest in the charity's charitable purposes or where they have provided or offered/provided support to further those charitable purposes, and that he recipient was provided with a clear and free way to opt out at the time their details were collected and with each subsequent communication sent to them. At present this

will only apply to charities who fall within the meaning of the Charities Act 2011) and not not-for-profit organisations.

You can read the Amendments put forward here, and the DMA's announcement here

UK GOVERNMENT CONSULTATION ON NEW LEGISLATION TO COMBAT RANSOMWARE

On 14 January 2025, the UK Government announced new proposals to legislation to help combat ransomware by reducing money flowing to ransomware criminals, strengthening operational agencies, and enhancing the government's understanding of ransomware threats. The proposals are open for consultation until 8 April 2025.

You can read the Government's announcement here.

OFCOM INTRODUCES NEW AGE ASSURANCE MEASURES TO PROTECT CHILDREN

Ofcom has published important new age assurance guidance under the Online Safety Act (**OSA**). The guidance focuses on matters including safeguarding children by setting expectations around robust age assurance measures and comprehensive assessments of children's access to platforms.

Ofcom has introduced a range of strict deadlines for different providers, for example – pornography providers must have 'highly effective age assurance' measures in place by July 2025 to safeguard children. Providers who fall within the OSA's scope must urgently assess the guidance, review their obligations and take steps to comply, or they could face strict enforcement action. Ofcom's phased approach to the OSA seeks to provide clear compliance guidelines for platforms to comply with the OSA and ensure a safer online environment for all children and online users.

You can read Ofcom's announcement here and statement here.

ICO EXPANDS WEBSITE COMPLIANCE REVIEW

On 23 January 2025, the ICO announced that it aims to ensure that (as part of its 2025 strategy) the UK's top 1,000 websites comply with data protection laws. This follows on

from the ICO's investigations into 200 websites in 2024, in which 134 organisations were sent communication about concerns with their cookie practices. The ICO has committed to setting out clear regulatory expectations that websites must provide their users with meaningful choices about the processing of their information. Stephen Almond, ICO Executive Director of Regulatory Risk emphasised the need for meaningful choices given how intrusive tracking can be on the most private parts of individuals' lives, (e.g. in the gambling sector where addicts are targeted). The ICO announced its commitment to providing guidance, advice and targeted enforcement.

You can read the ICO's announcement here.

ICO FINES ESL CONSULTANCY £200,000 FOR UNLAWFUL DIRECT MARKETING

The ICO imposed a £200,000 fine against ESL Consultancy Services Ltd for unlawfully sending direct marketing promotion messages to individuals. Approximately 38,000 complaints were made following the unsolicited communication, revealing that individuals had not consented to receive these messages. The ICO's investigation into the matter uncovered that deliberate attempts were made at bypassing consent obligations. In addition, the ICO has issued an enforcement notice, signifying the strong stance it takes against unlawful marketing practices. Businesses must ensure they obtain any legally required consents for marketing communications, be transparent about their data handling practices and maintain clear records to help demonstrate compliance.

You can read the ICO's announcement here.

UK GOVERNMENT ANNOUNCES INITIATIVE TO MODERNISE PUBLIC SERVICES

The UK Government announced its new technology and AI strategy to streamline public services, reduce delays and administrative time wasting and cut costs of taxpayers. This initiative includes AI tools coined the name "Humphrey" to speed up Whitehall work and to deliver better public services.

You can read the Government's announcement here.

OFCOM FINES MINTSTAR FOR FAILING TO PROTECT CHILDREN FROM HARMFUL CONTENT

On 23 January 2025, Ofcom fined MintStars Ltd (a video sharing platform) £7,000 for failing to protect under 18s from accessing pornographic content between November 2023 and August 2024. MintStar had relied on inadequate measures, such as self-declaration and disclaimers, instead of implementing robust age verification mechanisms. MintStars have cooperated with Ofcom during this investigation and have taken remedial action to implement age assurance technology.

You can read Ofcom's announcement here.

DIST PUBLISHES CODE OF PRACTICE ON AI CYBER SECURITY

On 31 January 2025, the Department for Science, Innovation and Technology (**DSIT**) published a Code of Practice on AI cyber security, focusing on the baseline principles to ensure secure AI systems during its lifecycle, addressing the risks posed to citizens and the digital economy, and create a global standard in the European Telecommunication Standards Institute.

You can read the DSIT's announcement here.

ICO ADDRESSES MISCONCEPTIONS ABOUT AI

On 28 January 2025, the ICO addressed the misconceptions about the use of AI and its concerns with data protection and privacy, affirming that individuals do retain control over their personal information. Individuals still have the rights over how their information is used to develop AI and, in many cases, can object to the processing. The ICO also addressed that AI developers are still required to be transparent about their processing, and even if these developers do not intend to process data, they still require a lawful basis for processing.

You can read the ICO's announcement here.

EUROPEAN UNION

CJEU ORDERS EUROPEAN COMMISSION TO COMPENSATE FOLLOWING UNLAWFUL TRANSFERS OF DATA

On 8 January 2025, the Court of Justice of the European Union (**CJEU**) ordered the European Commission to pay damages to visitors of its Conference on the Future of Europe website. This followed a compliant by a German citizen that the Commission unlawfully transferred his personal data to Meta Platforms via the "Sign in with Facebook" hyperlink on the EU Login Page.

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

EDPB PUBLISHES GUIDELINES ON PSEUDONYMISATION

On 17 January 2025, the European Data Protection Board (**EDPB**) published guidelines on pseudonymisation, clarifying the definition, its applicability, its advantages, and emphasising its role as an effective measure to meet data protection obligations. The guidelines are open for public consultation under 28 February 2025.

You can read the EPDB's announcement here, and the guidelines here.

EDPB ISSUES PAPER ON INTERPLAY BETWEEN DATA PROTECTION AND COMPETITION LAW

On 17 January 2025, the EDPB adopted a position paper on the interplay between data protection and competition law. This follows the CJEU ruling in Meta v Bundeskartellamt which indicated the need for data protection and competition law enforcement authorities to collaborate. The paper examines how the two interact and proposes recommendations for incorporating market and competition practices into data protection and enhancing regulatory cooperation through a possible single point of contact to manage coordination between regulators.

You can read the EDPB's announcement here, and the statement here.

EUROPEAN COMMISSION'S PLAN FOR STRENGTHENING CYBERSECURITY IN HEALTHCARE

On 15 January 2025, the European Commission revealed the "EU Action Plan" to enhance the cybersecurity resilience of hospitals and healthcare providers. This aims to improve the detection of threats, preparedness and response capabilities of hospitals and health providers to create a safer environment.

You can read the Commission's announcement here.

COMMISSION INVESTIGATIONS INTO X'S RECOMMENDER SYSTEM UNDER DSA

On 17 January 2025, the Commission announced that it has taken further investigatory measures against X's recommender system under the Digital Services Act (**DSA**). The Commission has requested X to supply internal documentation on its recommender systems, alongside recent updates by 15 February 2025. A retention order has been issued which requires X to preserve its internal documents on future changes and functioning of its algorithms until 31 December 2025.

You can read the Commission's announcement here.

EDPS NOTE ON DIGITAL CLEARINGHOUSE TO STRENGTHEN EU DIGITAL REGULATION

On 15 January 2025, the European Data Protection Supervisor (**EDPS**) announced it has published a concept note on Digital Clearinghouse 2.0, setting out the EDPS' proposal for improving cooperation and coherency in enforcing EU digital markets regulation. As the EU introduces the Digital Markets Act and the AI Act, the EDPS has emphasised the need for collaboration to avoid inconsistencies in application of the legal requirements and ensure that the rights and freedoms of individuals are respected. The proposed Digital Clearinghouse 2.0 is a forum dedicated to address regulatory

concerns and the EDPS notes that this should have adequate resources including a permanent secretariat.

You can read the EDPS' announcement here.

EDPB PUBLISHES REPORT ON THE RIGHT OF ACCESS

On 20 January 2025, the EDPB published a report "on the implementation of the right of access by controllers" evaluating how organisations implement the right of access, summarising the coordinated national actions in 2024 under the Coordinated Enforcement Framework (**CEF**). One of the findings of the report shows that awareness of the EDPB Guidelines 01/2022 on the right of access was significantly needed. Key challenges that were identified from the CEF action were the lack of documented procedures and inconsistent application of access requests limitations.

You can read the EDPB's announcement here, and the Report here.

NOYB FILES COMPLAINT AGAINST SEVERAL ONLINE SERVICE PROVIDERS FOR TRANSFERS TO CHINA

On 14 January 2025, Noyb filed GDPR complaints against TikTok, AliExpress, SHEIN, Temu, WeChat and Xiamoi for unlawfully transferring Europeans' personal data to China with no adequate safeguards in place.

You can read Noyb's announcement here.

EU AI ACT FIRST RULES TAKE EFFECT

On 3 February 2025, the European Commission announced that the key rules under the AI Act are in effect, including the AI system definition, literacy initiatives and providing a very limited list of prohibited AI uses posing unacceptable risks. The Commission will issue guidelines on AI systems definition, produce a repository of AI literacy practices and publish guidelines on the prohibited AI practices.

You can read the Commission's announcement here.

AUSTRIA

DSB CONCLUDES 2024 AUDIT AS A SUCCESS AND DETAILS PLANS FOR 2025

The Austrian Data Protection Authority (**DSB**) concluded its 2024 audit of the telecom sector with positive outcomes. The review focused on right of access, aligning with the CEFs right of access coordination action in 2024. In 2025 the DSB will focus on the right of erasure, although the sector of focus has yet to be announced.

You can read the DSB's announcement here.

AZOP REQUESTS ACTION OVER DISCLOSURE OF

CROATIA

SERBIAN DPA UNLAWFUL CROATIAN DATA

On 17 January 2025, Croatia's Data Protection Authority (**AZOP**) requested that the Serbian Commissioner for Information of Public Important and Personal Data Protection address and investigate the unlawful publication of Croatian citizen's personal data in a Serbian media outlet. This involved the media outlet exposing ID cards on screen during a live broadcast.

You can read the AZOP's announcement here.

CZECH REPUBLIC

UOOU WARNS OF CATALOGUE FRAUD AND IMPOSES SANCTIONS

In December 2024, the Office for Personal Data Protection (**UOOU**) warned organisations against the deceptive practices of catalogue fraud, which involves sending fraudulent invoices via email for unrequested services. The UOOU imposed a total fine of CZK 5 million on three companies for such practices and continues to investigate other companies. Businesses are urged not to pay these fraudulent invoices.

You can read the UOOU's announcement here.

DENMARK

DATAILSYNET PLAN FOR 2025

On 7 January 2025, Denmark's Data Protection Authority, the Datatilsynet, unveiled its focus areas for 2025 covering topics such as children's data protection, digital tracking, the right to erasure, AI and compliance with the Law Enforcement Act. These focus areas look to address complaints made to the Datailsynet and other relevant input.

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

DATAILSYNET APPROVES F.C. COPENHAGEN'S USE OF FACIAL RECOGNITION

On 16 January 2025, the Datatilsynet approved FC. Copenhagen's use of facial recognition at football matches to support the enforcement of its rules on club quarantines and suspensions where an individual has violated the rules of the club. This approval requires the football club to conduct a Data Protection Impact Assessment prior to its use and must strictly comply with the Danish Television Surveillance Act. Facial recognition may only be used for football matches and not for other events that may take place at the stadium, as it would not be considered necessary for the public interest.

You can read the Datailsynet's announcement here.

DATAILSYNET INVESTIGATES ALLES LAEGEHUS FOLLOWING DATA BREACH

On 23 January 2025, the Datailsynet, following several complaints and reports regarding a data breach, announced that it is investigating Alles Laegehus (a medical centre). It is focusing on assessing whether adequate security measures were in place, and whether the rules regarding notification to the Datatilsynet and the affected data subjects were followed correctly.

You can read the Datailsynet's announcement here.

ESTONIA

ESTONIA AKI FINES ASPER BIOGENE OU €85,000 FOR LACK OF APPROPRIATE SECURITY MEASURES

On 10 January 2025, the Estonian Data Protection Authority (**AKI**) imposed a fine of €85,000 against Asper Biogene OU following a data breach in 2023 which exposed sensitive information, such as genetic and health data. It was found that the company failed to implement appropriate security measures for processing personal data. The company was also found to have appointed a Data Protection Officer (**DPO**) with a conflict of interest, failing to adhere to the independence and competence required of a DPO. The fine is not finalised and can be appealed.

You can read the AKI's announcement here.

FINLAND

FINLAND'S OMBUDSMAN FINES SAMBLA GROUP

In December 2024, the Finnish Data Protection Ombudsman (**Ombudsman**) imposed a fine against Sambla Group of €950,000 for the company's poor data security, resulting in the unauthorised access to customers' loan application data via unsecured personal links. These links were exploited by phishing, exposing personal data such as financial details and marital status. The DPA ordered the company to stop processing personal data immediately and notify their affected customers. The company has since stopped using URL links and improved its security measures.

You can read the Ombudsman's announcement here.

OMBUDSMAN INVESTIGATES VALIO DATA BREACH

On 27 January 2025, the Finnish Ombudsman announced that it is currently investigating a personal data breach that occurred at Valio and its subsidiaries in Finland in December 2024. The Ombudsman's investigation aims to determine whether all companies affected by the breach complied with the applicable data protection laws.

You can read the Ombudsman's announcement here.

FRANCE

CNIL IMPOSES €240,000 FINE ON KASPR FOR UNLAWFUL DATA COLLECTION

In December 2024, the French Data Protection Authority, the CNIL, imposed a fine of €240,000 on KASPR (a paid extension for Chrome) for extracting contact details listed on LinkedIn and violating fundamental principles of the GDPR. This included the failure to obtain a valid legal basis for processing for violating LinkedIn's users' visibility preferences, disproportionate data retention practices, lack of transparency, and failure to comply with individual rights requests. KASPR is required to stop processing the contact details of LinkedIn users' who have limited their visibility on LinkedIn, cease the automatic renewal of retention, and ensure they respond to individuals' requests for their information. The company has 6 months to comply.

You can read the CNIL's announcement here.

CNIL PUBLISHES RECOMMENDATIONS ON RESPECTING USER PRIVACY

On 14 January 2025, the CNIL published its final recommendations on respecting user privacy to help mobile application developers design privacy friendly apps, with a focus on access permissions. Permission allows users to decide which apps have access to their device functionalities such as location, camera, audio or contacts. Permissions do not substitute "consent" under the meaning of GDPR. The CNIL advises app developers to select the least intrusive permissions and ensure a clear distinction between permission requests and the collection of consent, for transparency with users.

You can read the CNIL's announcement here.

CNIL PUBLISHES PRACTICAL GUIDE ON TRANSFER IMPACT ASSESSMENTS

In January 2025, the CNIL published a practical guide on transfer impact assessments to help organisations in ensuring the safe transfer of personal data to a third country outside the EEA, excluding those covered by an adequacy agreement. This guide aims to help organisations carry out their transfer impact assessments and is organised in six helpful steps.

You can read the CNIL's guidance here.

IRELAND

EU GENERAL COURT ORDERS DPC TO INVESTIGATE NOYB COMPLAINT

On 29 January 2025, the EU General Court held that the Irish Data Protection Commission (**DPC**) acted unlawfully when it refused to investigate a complaint by Noyb regarding Meta's use of personal data for advertising without consent. The EDPB in 2022 decided that the DPC should have investigated Meta's use of sensitive data, however the DPC rejected this and sued the EDPB. The General Court has dismissed the DPC's claims. The case will now be appealed to the CJEU.

You can read Noyb's announcement here and the court's judgment here.

ITALY

GARANTE FINES ILLUMIA €678,897 FOR UNLAWFUL TELEMARKETING PRACTICES

In December 2024, the Italian Data Protection Authority, the Garante, imposed a €678,897 fine on Illumia (an electricity and gas service company) for unlawfully processing personal data for the purposes of direct marketing. The Garante has required that Illumia implement technical and organisational measures to control external telemarketing agencies, to prevent unauthorised promotional marketing calls, and Illumia must address the risks of supply contracts entered following such unlawful practices.

You can read the Garante's announcement here.

GARANTE IMPOSES FINE OF €25,000 ON UNIVERSITY HOSPITAL FOR FAILING TO IMPLEMENT ADEQUATE SECURITY MEASURES

The Garante has imposed a €25,000 fine on University Hospital following their failure to implement appropriate security measures, which led to a ransomware attack compromising employee, consultant and patient data. The hospital was also found to have failed to use multi-factor authentication for VPN access and inadequate network segmentation that could help avoid the propagation of viruses.

You can read the Garante's announcement here.

GARANTE CEASES DEEPSEEK ACTIVITES OVER DATA PROTECTION CONCERNS

On 28 January 2025, the Garante sent an information request to Hangzhou and Beijing DeepSeek AI asking for confirmation on their current practices of collecting data, detailing the sources from which data is collected, its purposes for processing, its legal basis for processing and whether the information is stored in servers located in China. Following this request, the Garante on 30 January 2025 urgently ordered the restriction of the DeepSeek's processing of Italian users' data with immediate effect. Although DeepSeek have argued that they do not operate in Italy and that European legislation does not apply to them, the Garante found that DeepSeek's response to its request was insufficient and therefore imposed an immediate limitation and has launched an investigation.

You can read the Garante's announcement here.

GARANTE FINES E.ON ENERGIA SPA €890,000 FOR UNLAWFUL TELEMARKETING PRACTICES

On 31 January 2025, the Garante announced that it imposed a €892,738 fine against E.ON Energia Spa for its unlawful telemarketing practices, including mismanagement of consent and for the unauthorised use of data from a Facebook campaign. The Garante's investigation uncovered that consent was transcribed incorrectly by an employee and there were insufficient verification methods, which led to processing the data without a lawful basis. It was also found that data collected during a Facebook campaign was misused for telemarketing purposes without checking the origin of the data. The company also failed to comply with data right requests.

You can read the Garante's announcement here.

GARANTE ISSUES FINES OF €10,000 TO THREE ENTITIES

On 31 January 2025, the Garante announced that it fined Molise Region, Molise Dati Company and Engineering Ingegneria Informatica Spa €10,000 each for a data breach that occurred in 2022 in the FSE regional portal. A vulnerability in its IT system led to the unauthorised access to sensitive health information of several individuals. The companies failed to implement adequate system checks and access controls.

You can read the Garante's announcement here.

LITHUANIA

VDAI FINES THE EMPLOYMENT SERVICE FOR DATA BREACH

On 21 January 2025, the Lithuanian State Data Protection Inspectorate (**VDAI**) imposed a €9,000 fine against the Employment Service under the Ministry of Social Security and Labour following a data breach which disclosed the personal information of over 29,600 individuals. Due to a human error, an excel spreadsheet containing personal data was attached to a letter sent to nearly 300 clients. The VDAI found that the Employment Service failed to implement appropriate technical and organisational data protection measures and inform its staff regarding data security procedures, breaching GDPR.

You can read the VDAI's announcement here.

MALTA

IDPC REPRIMANDS CONTROLLER FOR FAILING TO GRANT A DATA SUBJECT ACCESS REQUEST

Malta's Office of the Information and Data Protection Commissioner (**IDPC**) reprimanded a controller for failing to grant a data subject access request to internal emails that included the data subject's data, as well as further information of processing activities. The IDPC emphasised that the right to access applies to all personal data, even if this is found in internal communications between employees.

You can read the IDPC's announcement here.

NETHERLANDS

AP FINES COOLBLUE €40,000 FOR UNLAWFUL COOKIE PRACTICES

On 24 December 2024, the Dutch Data Protection Authority (**AP**) imposed a €40,000 fine on Coolblue for unlawfully collecting personal data through cookies without users' consent, assuming visitors of their website agreed and used pre-ticked boxed. The AP began its investigation into the matter in 2019 and made recommendations to Coolblue, however the company failed to adopt correction measures until mid-2020. Following this fine, the AP has also provided clear rules for the use of cookies and appropriate designs of cookie banners, which can be accessed here. In addition, the AP has initiated a "cookie campaign" to raise awareness and for companies to review their current cookie policies.

You can read the AP's announcement here.

POLAND

UODO PRESIDENT SUBMITS COMMENTS ON DRAFT ACT ON AI SYSTEMS

On 16 January 2025, the Polish Data Protection Authority (**UODO**) submitted comments on the Draft Act on AI Systems, addressing the need for significant change and adaption of the GDPR provisions. The President of the UODO also highlighted that the act does not appear to appropriately reflect his role as the market surveillance authority (as

required by Article 74(8) of the EU AI Act) which needs to be addressed to avoid non-compliance. Other concerns were raised to ensure that the Draft Act complies with the EU AI Act and GDPR.

You can read the UODO's announcement here.

UODO FINES TOYOTA BANK POLSKA FOR VIOLATIONS OF GDPR

On 20 January 2025, the UODO fined Toyota Bank Polska SA PLN 576,220 for failing to properly register their data profiling activities within their record of processing activities, failing to assess its impact on data protection and for undermining the independence of its DPO.

You can read the UODO's announcement here.

SPAIN

AEPD ANNOUNCES SUPPORT OF WORLDCOIN'S ORDER TO DELETE IRIS DATA

In December 2024, the Spanish Data Protection Authority (**AEPD**) announced its support for the BayLDA ruling that the Worldcoin project violated the GDPR and therefore Worldcoin is required to delete all iris data collected unlawfully, those which were stored without the necessary security measures and must now gain explicit consent for any future processing of biometric data. AEPD has actively cooperated with the DPA under Article 60 GDPR. Fines and sanctions are expected to be issued for prior breaches.

You can read the AEPD's announcement here.

SWEDEN

IMY ISSUES REPRIMANDS AGAINST COMPANIES USING META PIXELS

In December 2024, the Swedish Data Protection Authority (**IMY**) completed its investigation into Apotea Sverige Ab, Länsförsäkringar AB (and its 27 subsidiaries companies) following their mistaken transfer of data to Meta through the use of Meta Pixels. This involved the unlawful transfer of personal data when a sub-function in the meta pixel was activated by mistake, highlighting the need for stricter technical and organisational security measures to be put in place. The IMY concluded that the

companies violated the GDPR and issued a reprimand. It was deemed a minor violation and therefore would not constitute the need to issue a fine.

You can read the IMY's announcement here.

IMY PUBLISHES NATIONAL GUIDANCE FOR AI USE IN PUBLIC ADMINISTRATION

On 21 January 2025, the IMY published guidance on AI in public administration to promote the safe and trustworthy use of AI and ensure the implementation of privacy by design.

You can read the IMY's announcement here, and the guidance here. (In Swedish only).

LIECHTENSTEIN

DPA GUIDES ORGANISATIONS ON REDACTION

On 15 January 2025, Liechtenstein's Data Protection Authority (**DPA**) published a reminder to organisations to ensure that redactions are used before publishing or passing on personal data. The DPA emphasises the need to properly redact, in a technically correct manner, to ensure that the information cannot be reconstructed.

You can read the DPA's announcement here and the guidance on redaction here.

NORWAY

NORWAY'S NEW APPROACH TO COOKIES

From 1 January 2025, a new e-communications law enters into force which requires that cookies and similar technology obtain valid consent under the GDPR, which will align national law with EU standards. The Norwegian Data Protection Authority (**DPA**) and the National Communications Authority will jointly oversee compliance with this new law and provide guidance.

You can read the DPA's announcement here.

BERMUDA

PRIVACY COMMISSIONER PUBLISHES GUIDANCE ON FEES FOR PIPA RIGHTS REQUESTS

Bermuda's Privacy Commissioner (**PrivCom**) published guidance on whether organisations can ask for a fee when responding to an individual's rights requests under the Personal Information Protection Act (**PIPA**) regarding the access to their data and medical information. Under PIPA organisations can charge a reasonable fee subject to limitations such as the maximum set by the Minister, no fee can be charged for the correction of an error. The PrivCom has suggested that imposing a fee may become a barrier to individuals' being able to exercise their privacy rights, and therefore the Government is developing a fee schedule however this has not officially been scheduled in time for the PIPA's entry into force on 1 January 2025.

You can read the PrivCom's guidance here.

TURKEY

KVKK PUBLISHES GUIDELINES ON PERSONAL DATA TRANSFERS

On 2 January 2025, the Turkish Data Protection Authority (**KVKK**) published guidelines on the transfer of personal data abroad, to assist data controllers with complying with Article 9 of the Law on the Protection of Personal Data No. 6698.

You can read the KVKK's announcement here, and the guidelines here (only available in Turkish)

CANADA

COMMISSIONER INVESTIGATES DATA BREACH AT POWERSCHOOL IMPACTING SCHOOLS

On 20 January 2024, the Canadian Privacy Commissioner announced that is has launched an investigation into a data breach at PowerSchool, an education technology company providing services to schools across Canada.

You can read the Commissioner's announcement here.

UNITED STATES OF AMERICA

NEBRASKA ATTORNEY GENERAL ISSUES LAWSUIT AGAINST CHANGE HEALTHCARE FOR DATA BREACH

In December 2024, the Nebraska Attorney General (**AG**) filed a lawsuit against Change Healthcare for violating the Consumer Protection and Data Security Laws in relation to a substantial data breach that occurred in January 2024, exposing the personal protection health information of thousands of Nebraskans. Hackers acquired stolen employee credentials and infiltrated Change Healthcare's systems, which forced the shutdown of the company's operations. The AG alleges that Change Healthcare operated outdated and poorly secured IT systems, failed to detect a hacker's unauthorised access for over a week, delayed notifying consumers of the data breach around 5 months after the breach occurred, disrupted healthcare operations placed financial burdens on hospitals in Nebraska. The AG seeks damages, penalties and a court-ordered action for Change Healthcare to upgrade their security.

You can read the AG's announcement here.

FTC FINALISES ORDER AGAINST MOBILEWALLA FOR SELLING SENSITIVE LOCATION DATA

On 14 January 2025, the FTC announced that it finalised its order against Mobilewalla and imposed a ban from the company's ability to sell sensitive location data after allegations that the Mobilewalla failed to obtain informed consent from customers before tracking and selling their information.

You can read the FTC's announcement here.

FTC ACTS AGAINST GENERAL MOTORS AND ONSTAR FOR UNLAWFULLY SHARING DRIVERS' LOCATION

On 16 January 2025, the Federal Trade Commission (**FTC**) announced that it will take action against General Motors and Onstar for processing and sharing drivers' location and driving behaviour data without adequately informing them and obtaining their consent. The FTC's proposed order seeks to ban the companies from sharing their

customer sensitive geolocation and behavioural data with consumer reporting agencies, as well as providing customers transparency and choice to processing of data.

You can read the FTC's announcement here.

GODADDY REQUIRED TO ADOPT ROBUST INFORMATION SECURITY PROGRAM FOLLOWING FTC INVESTIGATION

On 15 January 2025, the FTC ordered GoDaddy to implement a robust information security program following the FTC's finding that the company failed to secure its website hosting services and protect its users against cyber-attacks. The FTC argues that GoDaddy misled its customers by representing that they had deployed reasonable security and complied with the EU-US and Swiss-US Privacy Shield Framework (the framework in place at the time of breach in 2019-2022). The company is now prohibited from making such misrepresentations and must also hire an independent third-party assessor to conduct a review of their information security program.

You can read the FTC's announcement here.

FTC FINALISES CHANGES TO COPPA RULE TO PROTECT CHILDREN

On 16 January 2025, the FTC finalised its amendments to the Children's Online Privacy Protection Act (**COPPA**) Rule, introducing stricter requirements for the processing of children's personal data and to provide tool to parents to control the sharing of data.

You can read the FTC's announcement here.

FTC IMPOSES $20 MILLION FINE AGAINST GENSHIN IMPACT MAKER OVER CHILDREN'S CONSENT VIOLATIONS

On 17 January 2025, the FTC imposed a $20 million fine against HoYoverse (the maker of Genshin Impact) following allegations of its violations of the children's privacy laws, failing to collect parental consent and misleading customers about the costs and odds of winning loot box prizes in the game by using deceptive marketing tactics. The FTC ordered the company to implement strict parental controls, improve their transparency around the loot box and ensure compliance with the COPPA.

You can read the FTC's announcement here.

TRUMP RESCINDS BIDEN'S AI SAFETY EXECUTIVE ORDER

Reuters reported that President Trump on 20 January 2025 rescinded Biden's AI safety executive order, which aimed to reduce the risks of AI to national security, the economy and public safety, by requiring developers to share results of their safety tests with the US government. Trump has argued that this order hindered innovation.

You can read Reuter's story here.

POTENTIAL CHANGES TO THE EU-US DPF ON THE HORIZON? TRUMP ADMINSTERS PCLOB MEMBER TERMINATIONS

On 27 January 2025, the US Privacy and Civil Liberties Oversight Board (**PCLOB)** announced that the new President has terminated the positions of three PCLOB members. Given that this Board oversee the EU-US Data Privacy Framework (**DPF)**, Noyb has reported that this casts doubts over the DPF, with the appointments bringing the number of required members below the threshold, unable to operate unless the individuals are replaced. The EU have relied on the PCLOB to allow data to move freely, with adequate protection. This removal of members threatens the framework.

You can read the Reuters' announcement here, and Noyb's opinion here.

TEXAS SUES TIKTOK FOR MISLEADING CHILD SAFETY CLAIMS

On 7 January 2025, the Texas' Attorney General (**AG**) sued TikTok for misleading its app as safe for minors, whilst it exposed children to explicit content. TikTok claimed that graphic videos were infrequent and mild, which the AG argues that this was said to mislead parents and maintain its current age rating on app stores. Investigations revealed that these videos were not infrequent and can be easily accessible to minors. This follows the AG's previous lawsuit against TikTok for violating the Securing Children Online Through Parental Empowerment Act.

You can read the AG's announcement here.

TEXAS ATTORNEY GENERAL SUES ALLSTATE FOR UNLAWFULLY PROCESSING AND SHARING OF DATA

On 13 January 2025, Texas' Attorney General field a lawsuit against Allstate and Arity, its subsidiary, for unlawfully processing and selling driving data, including location and movement of telephone data of Texans through its embedded software in apps such as Life360. Allstate paid software providers to install its tracking software and then sold this information off to insurance companies without informing or obtaining consent of the individuals. This violated the Texas Data Privacy and Security Act (**TDPSA**), as no clear notice was provided, and no consent was obtained for the processing of sensitive information (which includes geolocation information). This is the first filed enforcement action under the TDPSA by the AG.

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

NEW YORK AG SECURES $450,000 SETTLEMENT FROM HOME SECURITY SURVEILLANCE PROVIDERS OVER DATA BREACH

On 28 January 2025, the New York AG secured a $450,000 settlement from Fantasia Trading LLC, Power Mobile Life LLC, and Smart Innovation LLC following their failure to adequately secure consumers' private footage from the home security cameras supplied to them. The AG found that the video streams were not securely encrypted and could be accessed by anyone with the link without need for authentication, which compromised on users' privacy. The companies are required to improve their current security measures to ensure data protection.

You can read the FTC's announcement here.

NEW YORK FINES PAYPAL FOR CYBERSECURITY FAILURES

On 23 January 2025, the New York Department of Financial Services imposed a $2 million fine against PayPal for its failure to safeguard and implement appropriate cybersecurity measures to protect consumers' personal information between 2017 and 2023. The Department's investigation revealed that untrained staff were in charge of implementing new system changes without proper procedures in place, which resulted in unauthorised access of sensitive customer information including social security numbers being exposed to cybercriminals. PayPal failed to implement and maintain written policies on use of access controls, identity management, and cybersecurity measures to protect personal data. Since the investigation, PayPal has improved their cybersecurity measures.

You can read the Department's announcement here.

CALIFORNIA ATTORNEY GENERAL REMINDS CONSUMERS ABOUT THE RIGHT TO OPT OUT OF THE SALE OF THEIR INFORMATION

On 29 January 2025, the Californian Attorney General reminded consumers of their right under the California Consumer Protection Act to opt out of the sale and sharing of their personal information and provided methods such as the Global Privacy Control browser setting to ensure these rights are in place and respected.

You can read the AG's announcement here.

OREGON DOJ PUBLISHES NEW PRIVACY TOOLKIT

On 28 January 2025, Oregon's Department of Justice launched a new toolkit to help residents protect their personal information and understand their privacy rights under the Oregon Consumer Privacy Act, which entered into force July 2024.

You can read the DoJ's announcement here

ARGENTINA

AAIP EMPHASISES IMPORTANCE OF PRIVACY POLICIES

On 28 January 2025, Argentina's Public Information Access Agency (**AAIP**) emphasised the importance of individuals reading privacy policies to understand the use of their data, rights and security measures. This highlights the fact

that organisations should ensure their privacy policies are up to date and easy for users to read and compliance with applicable data protection laws.

You can read the AAIP's announcement here.

BRAZIL

BRAZIL'S ANPD SUSPENDS TOOLS FOR HUMANITY'S ABILITY TO PAY USERS FOR IRIS DATA COLLECTION

On 24 January 2025, the Brazilian Data Protection Authority (**ANPD**) announced that it has placed a preventive measure on Tools for Humanity (**TFH**) suspending it from offering cryptocurrency or any other financial compensation to users for the collection of iris data. TFH, the parent company of Worldcoin, were found to have provided monetary incentives to users in exchange for iris data, which could compromise the ability for users to provide free and informed consent without being unduly influenced. The ANPD considered the sensitive nature of the processing and the seriousness of the impact on individuals and imposed a preventive measure on TFH.

You can read the ANPD's announcement here.

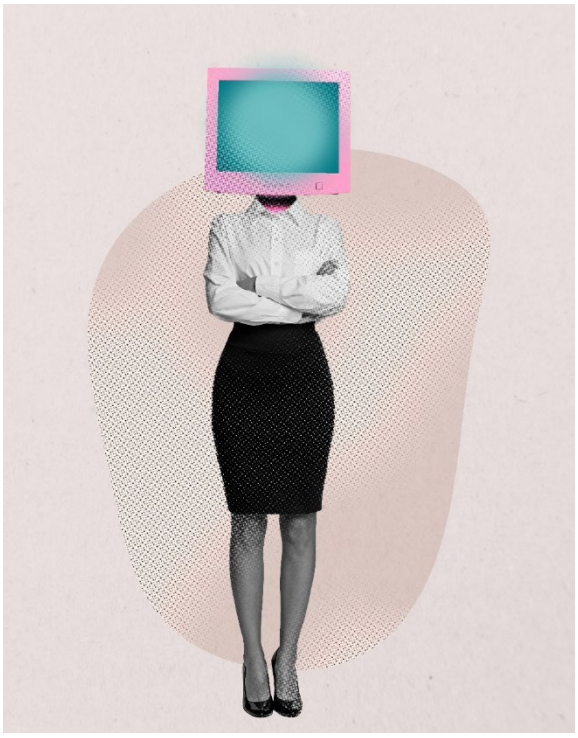
REPUBLIC OF SOUTH KOREA

PIPC GUIDELINES ON SAFE USE OF SYNTHETIC DATA

In December 2024, South Korea's Personal Information Protection Commission (**PIPC**) issued guidelines on generating and utilising synthetic data in a safe way to ensure protection of privacy. Synthetic data is data generated by AI computer simulation or algorithms, mirroring real-word data to meet specific needs.

You can read the PIPC's announcement here.

SOUTH KOREA'S NATIONAL ASSEMBLY PASSES ACT ON AI



In December 2024, South Korea's National Assembly passed the Basic Act on the Development AI and the Establishment of Trust, set to take effect in January 2026. This legislation aims to enforce rigorous requirements for high-risk AI systems.

You can read the announcement here, and the Act here (only available in Korean)

PIPC PUBLISHES AI PRIVACY RISK MANAGEMENT MODEL FOR TRUSTWORTHY AI

On 19 December 2024, the PIPC introduced the AI Privacy Risk management Model to facilitate the AI-powered businesses to voluntarily manage the privacy risks that arise from the development and deployment of AI. The models providers procedures for AI privacy risk management, the types of potential AI privacy risks. Mitigation measures for these risks and a detailed framework for managing these risks.

You can read the PIPC's announcement here.

NATIONAL COURT ADMINISTRATION FINED BY PIPC FOR DATA BREACH

On 9 January 2025, the PIPC announced that it fined the National Court Administration KRW 213 million for failing to comply with the Personal Information Protection Act, which resulted in a breach. Hackers were able to exploit the unsecured portal to access the agency's electronic litigation servers within its internal network, which exposed sensitive litigation documents of just under 18,000 individuals. The PIPC's investigation revealed that the National Court had failed to implement robust security measures such as failing to encrypt litigation related documents, using weak passwords, and failed to install antimalware and other required security programs on its server.

You can read the PIPC's announcement here.

PIPC AND CPPA COLLABORATE TO PROMOTE DATA PROTECTION

On 12 January 2025, the PIPC and California Privacy Protection Agency (**CPPA**) announced that they signed a declaration of cooperation to improve cross-border collaboration on privacy and data protection matters.

You can read the PIPC's announcement here.

PIPC FINES KAKO PAY, APPLE AND ALIPA FOR PRIVACY VIOLATIONS

On 23 January 2025, the PIPC fined Kako Pay, Apple and Alipay for transferring personal data across borders without complying with the Personal Information Protection Act. Kako Pay was fined KRW 5.97 billion for failing to obtain consent before sharing user data with Alipay, Apple was fined KRW 2.4 billion for failing to inform users about cross border transfers and Alipay received a corrective order notice requiring it to dismantle its customer specific score which was built using data that was obtained unlawfully.

You can read the PIPC's announcement here.

SINGAPORE

PDPC ISSUES 3 UNDERTAKINGS

In January 2025, the Personal Data Protection Commission (**PDPC**) issued three undertakings following ransomware attacks exposing the personal data of over 14,477 individuals due to inadequate security measures e.g. poor access controls and weak password security. The organisations involved are required to implement corrective measures, including mandating single sign-on with two factor authentication, encrypting data, improved threat detection and training staff on security procedures.

You can read the PDPC's announcement here.

NEW ZEALAND

OPC ANNOUNCES PROGRESS OF PRIVACY AMENDMENT BILL

On 31 January 2025, New Zealand's Office of the Privacy Commissioner (**OPC**) announced that the Privacy Amendment Bill is progressing through Parliament and has produced information to update organisations. The Commissioner will develop guidance on the important changes proposed by the Bill and review the existing Codes of Practices

to assess necessary amendments. The proposed timeline is expected to be ahead of the Bill's implementation, scheduled for 6 months after its passage.

You can read the OPC's announcement here.