



## UK REGULATOR ICO INVESTIGATES TIKTOK, REDDIT AND IMGUR REGARDING ITS PROCESSING OF CHILDREN'S DATA

On 3 March 2025, the Information Commissioner's Office (**ICO**) launched an investigation into TikTok, Reddit and Imgur with the aim of establishing whether these online platforms breached data protection laws when handling and processing personal data of 13–17-year-olds.

The investigation into TikTok follows growing concerns regarding its use of children's data to influence their recommender systems and algorithms, which could lead to children being exposed to harmful or inappropriate content.

The investigation into Imgur and Reddit is regarding their age verification measures and whether they adequately protect the personal information of children.

These investigations are part of the ICO's efforts to ensure social media and video sharing platforms comply with data protection legislations and Ofcom's Children's Code to protect children's privacy online.

You can read the ICO's announcement [here](#).

### PG. 5

OFCOM DRAFT GUIDANCE  
ON TACKLING ONLINE  
HARMS AGAINST WOMEN  
AND GIRLS

### PG. 8

CJEU RULES ON AUTOMATED  
CREDIT ASSESSMENTS

### PG. 19

KVKK PROVIDES GUIDELINES  
FOR SUBMITTING STANDARD  
CONTRACTS FOR DATA  
TRANSFERS

**UNITED  
KINGDOM****ICO PUBLISHES FREE DIRECT MARKETING COMPLIANCE TOOL**

On 5 February 2025, the ICO launched a new free direct marketing online tool to help organisations ensure their marketing practices comply with the UK GDPR and the Privacy and Electronic Communication Regulations (**PECR**).

Organisations can answer a few questions and receive the relevant guidance in one place, saving time on searching for the information themselves. The ICO has emphasised the importance of organisations complying with direct marketing rules, highlighting the fact that numerous fines were issued last year for failing to comply.

You can read the ICO's announcement [here](#), and the generator [here](#).

---

**COMMISSIONER'S RESPONSE TO AMENDMENTS TO THE DATA USE AND ACCESS BILL**

On 10 February 2025, the ICO's Commissioner announced its overall support for the amendments proposed to the Data Use and Access (**DUA**) Bill, which has completed its passage through the House of Lords. The Commissioner commented that the DUA Bill strengthens data protection, upholds people's rights, and allows for greater innovation. The ICO has welcomed the changes to the scientific research definitions and has offered that the ICO will provide guidance on what is meant by "public interest" for scientific research. The Commissioner supports the added protections provided to children, however, seeks clarity on the meaning of higher protection matters to ensure that there is no confusion between the protections of children data and that of adult data. As for the reported amendment on soft-opt in for charities, the ICO has announced support for this extension however urges charities to be careful when implementing this, balancing their interests with the individuals' rights and freedoms to avoid harm. The DUA sees significant changes in the way automated decision-making is to be approached, with a greater focus on removing restrictions to allow for innovation, subject to the need to implement appropriate safeguards. The ICO also considers other provisions dealing with web crawlers and deepfakes and seeks the government's clarity and reassurance. The ICO will continue to monitor debates and amendments and commits to issue independent guidance on its implementation.

You can read the ICO's announcement [here](#).

---

## OFCOM SUPPORTS SAFER INTERNET DAY FOCUSING ON COMBATTING ONLINE SCAMS

On 11 February 2025, UK's Office of Communications (**Ofcom**) expressed its commitment to support Safer Internet Day by focusing on combatting online scams, with the theme of this year being "too good to be true?". Studies show that 9 in 10 people within the UK encounter online scams or fraud, with over a quarter losing money consequently. These figures demonstrate the need for online safety and raising awareness. Ofcom, as part of its effort to strengthen online safety, has implemented new measures under the Online Safety Act to combat online fraud and improve reporting.

You can read the Ofcom's announcement [here](#).

## THE UK GOVERNMENT PUBLISHES A NEW AI PLAYBOOK

The UK Government has released its Artificial Intelligence Playbook. This document provides important guidance for civil servants and public sector organisations on using AI safely, effectively, and securely. It lays out ten key principles for AI use in government and offers practical advice on selecting, procuring and implementing AI solutions. The playbook explains AI's capabilities, limitations and risks, with the aim of helping civil servants assess whether AI is the right tool for their needs. It builds on the Generative AI Framework for HMG published in 2024 – yet now covering a wider range of AI technologies.

You can read the Government's announcement [here](#).

---

## UK SAFETY INSTITUTE BECOMES AI SECURITY INSTITUTE STRENGTHENING PROTECTION AGAINST NATIONAL SECURITY AND CRIME RISKS

On 14 February 2025, the UK Government announced that the AI Safety Institute has been rebranded as the AI Security Institute to focus on risks posed by AI to national security and crime such as cyber-attacks and fraud.

You can read the UK Government's announcement [here](#).

## UK GAMBLING FIRMS FOUND TO BE ILLEGALLY SHARING VISITOR DATA OVER FACEBOOK

On 8 February 2025, the Guardian reported that the *Observer* has revealed that several UK gambling firms are secretly tracking website visitors and transmitting their data to Meta through the Facebook platform without obtaining the consent of the users. This data is then used to profile individuals are gamblers, leading to targeted ads appearing on their screens. 52 out of the tested 150 were found to have automatically shared visitor data with Meta via their Pixel tracking tool. This is unlawful, as marketing requirements under PECR and UK data protection laws require the explicit consent from users.

You can read the Guardian's story [here](#).

## APPLE TO REMOVE DATA PROTECTION TOOL FOLLOWING GOVERNMENT'S DEMAND FOR DATA

On 21 February 2025, the BBC reported that Apple is removing its highest-level advanced data protection (**ADP**) tool from its UK customers following the Government's demand to access user's encrypted data under the Investigatory Powers Act. The ADP feature allowed for only the account holder to be able to access photos or documents on iCloud using end-to-end encryption. The UK government's request would require Apple to have created a back door into its encryption service, which Apple was not willing to provide. Apple's approach to remove the ADP has been met with concerns internationally, with US politicians warning that the UK's demands may jeopardise global data security, whilst those in the child safety sector have called for Apple to implement further measures to protection children from online abuse and safeguard their personal data.

You can read the story [here](#).

## DATA USE AND ACCESS BILL PROGRESSES THROUGH HOUSE OF COMMONS

On 12 February 2025, the House of Commons completed its second reading of the [Data Use and Access Bill](#). The line by line review is scheduled for 4 March 2025, in which the Bill will enter the Committee Stage.

You can track the progress [here](#).

## OFCOM DRAFT GUIDANCE ON TACKLING ONLINE HARMS AGAINST WOMEN AND GIRLS

On 25 February 2025, Ofcom introduced practical steps for online services to combat misogyny, harassment, domestic abuse, intimate image abuse and other harms. The draft guidance highlights the importance for online platforms to implement stronger security and safer default settings and addresses 9 areas which these platforms can do more to prevent harm. Technology firms are urged to take a more proactive responsibility for women and girl's online safety, with Ofcom set to monitor compliance and enforce action. The guidance is open to consultation until 23 May 2025.

You can read Ofcom's announcement [here](#), and the guidance [here](#).

---

## ICO ISSUES ENFORCEMENT NOTICE TO SMART HOUSE ENSURED LTD FOR MISUSE OF DATA FOR MARKETING PURPOSES

On 25 February 2025, the ICO issued an enforcement notice to Smart House Ensured Ltd for making 14,508 unsolicited telemarketing calls to subscribers who were registered on the Telephone Preference Service. This violates the Privacy and Electronic Communications Regulations 2003, which requires consent for telemarketing communications. For such communications to be valid the individual would need to take a proactive approach to override their TPS registration, which was not the case and therefore led to the enforcement notice from the ICO.

You can read the ICO's announcement [here](#).

## ICO REPRIMANDS SCOTTISH CITY COUNCILS FOR DELAYS IN RESPONDING TO INFORMATION REQUESTS

On 26 February 2025, the ICO reprimand Glasgow City Council and City of Edinburgh Council for repeatedly failing to meet its deadlines set by law to respond to subject access requests. The ICO commented that it is committed to monitoring local authorities proportionately.

You can read the ICO's announcement [here](#).

## ICO PUBLISHES GUIDANCE ON PROCESSING EMPLOYMENT RECORDS

On 5 February 2025, the ICO published guidance on the processing of employment records to help employers understand their obligations under the UK GDPR and Data Protection Act 2018 when handling employment records. It includes information on how to lawfully collect and process employees' personal data whilst ensuring compliance with data protection obligations.

You can read the ICO's announcement [here](#), and the guidance [here](#).

### EUROPEAN UNION

## EDPB FEBRUARY PLENARY UPDATES

On 12 February 2025, the European Data Protection Board (**EDPB**) adopted key measures during its February 2025 plenary meeting, including:

- A statement on age assurance, outlining 10 principles for ensuring a consistent approach across Europe to protect minors and comply with data protection requirements. The chair of the EDPB emphasised the need for age verification methods which are as less intrusive as possible to protect children for harmful content. You can read the statement [here](#).
- Expanding the scope of the ChatGPT task force to cover broader AI enforcement and support and coordinating Data Protection Authorities actions when dealing with AI complexities.
- Adopting recommendations on the 2027 WADA World Anti-Doping Code, which show the need for implementing safeguards and protecting the personal data of athletes, which in many cases will involve special category data. The EDPB aims to assess the Code alongside the GDPR to ensure compatibility.

You can read the EDPB's announcement [here](#).

## EUROPEAN COMMISSION REQUESTS INFORMATION FROM SHEIN UNDER THE DSA

On 6 February 2025, the European Commission announced that it requested information from Shein to provide internal documents and information on the risks associated with the presence of illegal content and goods on its store, to provide transparency on recommender systems and the access to data for qualified



researchers under the Digital Services Act (**DSA**). The Commission is also requesting information on the data protection measures in place for its users.

You can read the Commission's announcement [here](#).

---

## COMMISSION WITHDRAWS DRAFT PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATION AND AI LIABILITY DIRECTIVE

On 11 February 2025, the European Commission announced that it has withdrawn the draft regulation on Privacy and Electronic Communications, arguing that “no agreement is expected from the co-legislators” and that the regulation is outdated not aligning with recent developments in legislation. In addition, the AI Liability Directive was withdrawn with the Commission arguing “no foreseeable agreement,” however with the opportunity to table another proposal on the topic.

You can read the Commission's announcement [here](#) (page 26).

## EU'S INVESTAI INITIATIVE LAUNCHED

On 11 February 2025, the European Commission launched InvestAI, a €200 billion initiative to help boost the development of AI and make Europe a global leader in AI by fostering open, collaborative innovation. This includes a €20 billion fund for 4 AI gigafactories, aiming to training the most complex large AI models. InvestAI will leverage existing EU programs like Digital Europe and Horizon Europe.

You can read the Commission's announcement [here](#).

## COMMISSION EMPHASISES THE IMPORTANCE OF RESPONSIBLE USE OF INTERNET

On 11 February 2025, the European Commission reaffirmed its commitment to promote the online safety of users, especially minors, following Safer Internet Day. The commission emphasises the need for responsible internet use and will do so through actions such as enforcing DSA measures, creating guidelines for online platforms and ensuring the providers develop privacy friendly age verification. In addition, the Commission is launching AdWise Online Campaign to help young gamers recognise their rights and to be able to identify manipulative practices. The commission is also working on the Digital Fairness Act to prevent online exploitation.

You can read the Commission's announcement [here](#).

---

## CJEU RULES ON AUTOMATED CREDIT ASSESSMENTS

On 27 February 2025, the Court of Justice of the European Union (**CJEU**) ruled that individuals subject to automated decision making are required to receive an explanation allowing them to understand and challenge the decision that have been made against them. This case concerned a refusal by a mobile operator in Austria to allow a contract to a customer, based on an automated credit check carried out by Dun & Bradstreet Austria. The CJEU clarified that data controllers are to provide meaningful information regarding the decision-making process for automated decisions. It is not enough to disclose the algorithm use to meet transparency requirements. Controllers must provide the individual with sufficient information regarding how their personal information is used to influence the decision and there must be an opportunity for the data subject to challenge this.

You can read the CJEU's announcement [here](#).

## EUROPEAN PARLIAMENT PRODUCES REPORT ON ALGORITHMIC DISCRIMINATION UNDER EU LAW



On 26 February 2025, the European Parliamentary Research Service produced a report on the interplay between the EU AI Act and the GDPR, exploring the potential legal uncertainties that arise between the two, particularly in regard to the processing of sensitive personal data into AI systems whilst promoting AI innovation. The report highlights the types of AI systems likely to cause discrimination such as generative AI, autonomous cars, job recruitment and credit scoring and how the AI Act aims to regulate and mitigate this.

You can read the Parliament's Research Report [here](#).

---



**AUSTRIA****AUSTRIA DSB ANNOUNCES MONITORING OF DEEPSEEK**

On 11 February 2025, the Austrian Data Protection Authority (**DSB**), following increased inquiries about DeepSeek's AI chatbot, announced that they are in regular contact with EEA supervisory authorities and the EDPB, assuring users that it is closely monitoring developments. The DSB will update further should more information become available.

You can read the DSB's announcement [here](#).

**BELGIUM****BELGIAN DPA REPRIMANDS ANTWERP NOISE POLLUTION RESEARCH DATA COLLECTION**

On 18 February 2025, Belgium's Data Protection Authority (**DPA**) reprimanded the City of Antwerp for its 2022 research project on smart noise monitoring pilot in the student district. The project included the recording of 10 second audio clips and generated voice imprints, which were then used to train an AI model. The DPA investigations found that Antwerp City lacked a sufficient legal basis for processing, miscommunicated the extent of the data to be collected, and failed to sufficiently encrypt the data. This violated the GDPR, breaching the principles of transparency and lawfulness.

You can read the DPA's announcement [here](#).

---

**CROATIA****AZOP RAISES AWARENESS AROUND CHILDRENS' ONLINE SAFETY**

As part of the Croatian's Data Protection Authority (**AZOP**) approach to tackling Safer Internet Day, key reminders have been made available on its website on the importance of responsible use of digital technologies and the protection of personal data especially those of children. AZOP's highlights some key online threats to children, including cyberbullying, identity theft, inappropriate content, and fake profiles and scams.

You can read the AZOP's announcement [here](#).

---

**DENMARK****DATAILSYNET CRITICISES COMPANY FOR UNLAWFULLY PROCESSING EMPLOYEE PERSONAL DATA**

On 10 February 2025, Denmark's Data Protection Authority, the Datalysnet, criticised a company for unlawfully accessing and downloading emails from a former employee's private email account during an employment dispute. The company argued that they processed this information based on legitimate interests, using the emails to prosecute the complainant. The Datalysnet found however that the company's actions violated data protection laws, since the email account was personal and not work related.

You can read the Datalysnet's announcement [here](#).

---

**FINLAND****FINNISH OMBUDSMAN ANNOUNCES AUDIT PLAN FOR 2025**

On 11 February 2025, the Finnish Data Protection Ombudsman published its audit plan for 2025, focusing on personal data processing individuals cannot directly control, especially in security-related sectors.

You can read the Ombudsman's announcement [here](#).

**FRANCE****CNIL IMPOSES €40,000 FINE AGAINST REAL ESTATE COMPANY**

The French Data Protection Authority, the CNIL, imposed a €40,000 fine against a real estate company for unlawfully monitoring employees through software installed on computers to measure employee working time. This software recorded supposed inactivity and took regular screenshots of the computers, and was found to have no lawful basis for processing as it was disproportionate. In addition, employees were not informed of this processing, breaching the transparency requirement. The CNIL's investigations also revealed that the company was recording both images and audio of employees in the workplace. Given the severity of the breach of data protection laws, the CNIL revealed the fine, however the name of the company remains anonymous given its small size and the fact that it took immediate corrective action.

You can read the CNIL's announcement [here](#).

## CNIL PUBLISHES RECOMMENDATIONS ON AI AND GDPR

On 7 February 2025, the CNIL published two new recommendations for ensuring AI technologies protect personal data by complying with the GDPR. The recommendations propose solutions to inform individuals whose data is used in AI models, and to facilitate them experience their GDPR rights.

You can read the CNIL announcement [here](#).

## CNIL CLASSIFIES QWANT'S PROCESSING OF DATA AS FALLING UNDER THE DEFINITION OF PERSONAL DATA

On 11 February 2025, the CNIL decided that the data QWANT, a search engine, transmitted to Microsoft was in fact pseudonymised data and not anonymised, therefore constituting personal data. This meant a revision to the company's privacy notice was due. The company initially believed that the data collected was anonymised, but the CNIL ruled otherwise. The company has since updated their privacy notice, cooperated and implemented strong privacy safeguards, meaning the CNIL issued a reminder rather than imposing a fine.

You can read the CNIL announcement [here](#).

### GERMANY

## GERMAN AUTHORITIES INVESTIGATE DEEPSEEK

On 14 February 2025, the Baden-Wuerttemberg Data Protection Authority, alongside several other German state data protection supervisory authorities, initiated a coordinated investigation into DeepSeek. The Inquiry will focus on whether DeepSeek have appointed a nominated representative in the EU under Article 27 of the GDPR. The Baden-Wuerttemberg has published recommendations for AI providers outside the EU who have not appointed a legal representative in the EU [here](#).

You can read the DPA's announcement [here](#).

### GREECE

## GREEK DPA INVESTIGATES DEEPSEEK AND WHATSAPP DATA BREACH

On 6 February 2025, the Greek Data Protection Authority (DPA) announced that it has launched an ex officio investigation into the lawfulness of

DeepSeek under the GDPR. In addition, the DPA will also be investigating a personal data breach affecting Greek users of WhatsApp caused by malicious software.

You can read the DPA's announcement [here](#).

## GREEK DPA COMMENTS ON DRAFT REGULATION ON PERSONAL NUMBERS ON ID CARDS

On 12 February 2025, the Greek DPA announced that the Ministry of Digital Governance submitted a draft provision on the processing of personal numbers on identity cards and replacing photocopies with digital copies in the private sector. The DPA has agreed that provided risk mitigation measures are implemented, the current draft provisions do not conflict with the protection of individual's personal data. The legislation must include public awareness and ensure that the storage of biometric data is clearly distinguishable.

You can read the DPA's announcement [here](#).

---

### IRELAND

## DPC SUBMITS DRAFT DECISION ON INQUIRY INTO TIKTOK

On 24 February 2025, the Irish Data Protection Commission (DPC) submitted a draft decision regarding the inquiry into TikTok regarding EU/EEA user data transfers to China and whether TikTok is complying with its transparency responsibilities and data transfer requirements.

You can read the DPC's announcement [here](#).

## GOVERNMENT INTRODUCES NEW BILL REGULATING AI

On 18 February 2025, the Irish Government introduced the Regulation of Artificial Intelligence Bill which is designed to implement the EU AI Act establishing harmonised rules on AI. The Bill will establish national regulatory bodies responsible for implementing and enforcing the EU AI Act, overseeing compliance, risk assessment and impact evaluation. The Bill also aims to enforce penalties for companies failing to comply with the AI regulations.

You can read the Government's announcement [here](#) (page 16)

---

## ITALY

## GARANTE WARNS AGAINST PUBLISHING POLITICIAN'S CHAT

On 13 February 2025, the Italian Data Protection Authority, the Garante, issued a formal warning to Società Editoriale Il Fatto SPA addressing concerns over potential risks to individuals' privacy. The warning concerned the volume "Fratelli di chat" which publishes chats between Italian politicians, often with the excessive publication of quotation marks, which may violate data protection laws. According to Constitutional law, correspondence between parliamentarians, ministers and party leaders are legally comparable to private correspondence which determine an expectation of confidentiality. In addition, the excessive use of direct quotations may also breach the principle of essentiality of information. The Garante has launched an investigation into the matter.

You can read the Garante's announcement [here](#).

## GARANTE ISSUES WARNINGS AGAINST THOSE MISUSING GRAPHITE SPYWARE

On 14 February 2024, the Garante issued a warning against those who misuse spyware solutions (such as Graphite from Paragon Solutions Ltd and similar systems). This followed complaints from journalists and citizens about the misuse of the spyware and the potential for Italian citizens' privacy being violated. Graphite provides the ability to intercept messages from numerous encrypted messaging platforms such as WhatsApp without the user having to interact. It has been reported that around 90 users globally were affected. WhatsApp has since issued a cease and desist notice to the spyware company and has alerted the affected WhatsApp users of the possible compromise to their device. The Garante has stated that use of such spyware requires strict adherence to data protection laws. The Garante will take further action to identify and sanction those who misuse this spyware software, with the potential of enforcing a fine of up to €20 million or 4% of turnover.

You can read the Garante's announcement [here](#), and the warning [here](#).





## GARANTE FINES WIND TRE FOLLOWING UNLAWFUL TELEMARKETING PRACTICES

On 28 February 2025, the Garante announced that it imposed a €347,520 fine against Wind Tre for the misuse of personal data for the purposes of telemarketing and for failing to implement appropriate security safeguards. It found that the company had used contact lists that were illegally obtained from third party commercial partners, where no consent was obtained. The Garante received several reports of unwanted marketing calls.

You can read the Garante's announcement [here](#).

### LATVIA

## DVI DISCUSSES COMMON PRIVACY NOTICE MISTAKES

On 19 February 2025, the Latvian Data Protection Authority, the DVI, discussed the common issues found in privacy notices, calling for organisations to do better. For organisations to ensure transparency they must produce a privacy notice and publish this on their website to inform users about what data is collected and how it is used. You can read the DVI's guidance [here](#), its sample privacy notice [here](#), and a recording of a webinar [here](#).

You can read the DVI announcement [here](#).

### LITHUANIA

## VDAI CALLS FOR CAUTION WHEN USING DEEPSEEK

On 7 February 2025, the Lithuanian State Data Protection Inspectorate, the VDAI, cautioned users against the use of DeepSeek, as it closely monitors the situation in relation to DeepSeek's compliance with the GDPR. Key concerns include the lack of transparency regarding how personal data is processed, the use individuals' input, chat history and other content to improve their service through training, and the potential storage of data on Chinese servers.

You can read the VDAI's announcement [here](#).

### LUXEMBOURG

## CNPD ISSUES RECOMMENDATIONS REGARDING USE OF DEEPSEEK

On 3 February 2025, the National Commission for Data Protection (**CNPD**) warned users about the potential risks linked to DeepSeek AI, developed in China and available online to all users across the globe. It warns that the

software is not designed for European users. Key concerns include lack of transparency, legal uncertainty as no legal representative has been nominated in the EU, the risks involved with third party actors processing information, and the possibility that EU users may struggle to exercise their GDPR rights. The CNPD recommends not installing DeepSeek, not to enter confidential or personal data when using this model, to raise awareness with staff over the risks involved, and to ensure that when using AI tools the GDPR rules are followed.

You can read the CNPD's announcement [here](#).

## NETHERLANDS

### AP WARNS AGAINST DEEPSEEK USE

On 3 February 2025, the Dutch Data Protection Authority, the AP, like most EU data protection regulatory authorities, warned citizens of the use of the DeepSeek chatbot following concerns over privacy and how the company handles personal data. The AP notes that the personal data may be stored in China and therefore Dutch users' data may be transferred outside the EU without proper safeguards in place. The privacy notice provided by DeepSeek is unclear, failing to meet transparency clients and raises concerns over how data is processed and used. The AP has announced that it is launched a boarding investigation into the transfer of personal data to China and recommends that users think before sharing their data.

You can read the AP's announcement [here](#).

### AP CALLS FOR CAUTION OVER CHATBOT APPS USED FOR FRIENDSHIPS AND THERAPY

On 12 February 2025, the AP found that many AI powered chatbot apps, for virtual companionship and mental health support, were unreliable, harmful, misleading and often contain addictive elements. This follows the AP's latest AI and Algorithm Risks Report which investigated 9 popular chatbot apps. These chatbots were found to often provide harmful responses, especially around the topic of mental health. The AP raised concerns regarding the lack of transparency to users, especially in cases where individuals are disclosing highly sensitive information, and they are unclear regarding the chatbot's processing activities. Following the enactment of the EU AI Act, a ban will be imposed on manipulative and deceptive AI practices, bringing about unacceptable risks. Therefore, developers are required to assess the risks and ensure their AI model does not cause users harm, and users should be cautious over the use of AI for mental health concerns.

You can read the AP's announcement [here](#).

**POLAND****UODO COMMENTS ON THE LAWFULNESS OF BODY WORN CAMERAS**

On 5 February 2025, the Polish Data Protection Office (**UODO**) commented on the lawfulness of processing personal data by paramedics through the use of body worn cameras. The UODO emphasises the need for legal regulations and data protection impact assessments before introducing these cameras, as well as stressing the need for data retention and the purpose for processing to be strictly defined.

You can read the UODO's announcement [here](#).

---

**UODO UPDATES GUIDANCE ON PERSONAL DATA BREACHES**

On 20 February 2025, the UODO updated its guidance on personal data breaches to reflect current regulations, providing practical examples and case studies, guidelines for cooperation with the UODO and key recommendations for risk assessment and preventing data breaches. To support organisations further, the UODO aims to host a seminar on managing and reporting data breaches.

You can read the UODO's announcement [here](#).

---

**PORTUGAL****CNPD TO INCREASE PROTECTIONS FOR CHILDREN REGARDING VIOLENT CONTENT ONLINE**

On 11 February 2025, the Portuguese National Data Protection Commission (**CNPD**) announced its plan to protect children and young people from violent digital content. A new priority interaction channel will be created to allow children to report highly violent online content, especially those that seem to target minors and young women, which will be urgently looked at by the CNPD. The CNPD has also announced their support for the Government's recent recommendation on imposing restricting within schools regarding the use of mobile phones.

You can read the CNPD's announcement [here](#).

**SLOVENIA****IP JOINS EFFORTS TO REGULATE AI AND PROTECT PERSONAL DATA**

On 19 February 2025, the Slovenian Information Commissioner (**IP**) joined EU supervisory authorities in efforts to protect individuals' rights and freedoms when using generative AI models. The IP will look at the circumstances that require investigations against AI providers, with a focus on the potential impact of AI on vulnerable groups such as children and the elderly. The IP advises users to exercise caution when using AI tools and be mindful before entering personal data, assessing whether information will be used to train the AI.

You can read the IP's announcement [here](#).

---

**SWEDEN****IMY ISSUES GUIDANCE ON IMPACT ASSESSMENTS**

On 18 February 2025, the Swedish Data Protection Authority (**IMY**) issued guidance on conducting impact assessments, consisting of a practical guide and an annex with legal interpretation for support to help businesses better understand how to carry out impact assessments.

You can read the IMY's announcement [here](#).

**ICELAND****ICELAND'S DPA FINES PRIMARY HEALTH CARE FOR PROCESSING**

On 18 February 2025, the Iceland Data Protection Authority (**DPA**) imposed an ISK 5,000,000 fine on Capital Region Health Service following the unlawful handling of personal data within its joint medical record system and the sharing of this information with these organisations. It found that these organisations failed to comply with the legal requirements of the Medical Records Act and were fined for unlawfully providing access to their patient records.

You can read the DPA's announcement [here](#).

**NORWAY****NORWAY DPA PUBLISHES FAQs ON TRANSFERS OF DATA TO US**

On 26 February 2025, Norway's Data Protection Authority (**DPA**) published FAQs on the status of transfers of personal data to the US following changes in the membership of the US Privacy and Civil Liberties Oversight Board (**PCLOB**). The FAQs include information regarding the current adequacy decision, the functioning of the PCLOB, and the Commission's monitoring of events to decide whether the adequacy decision should remain and advice for businesses. Organisations are advised to prepare contingency plans in case future changes occur that will restrict data transfers to the US, and in the event this occurs it is unlikely for there to be a transition period. The DPA will continue to monitor this area and provide more information where needed.

You can read the DPA's announcement [here](#).

**GLOBAL****OECD PUBLISHES GLOBAL FRAMEWORK FOR AI REPORTING**

On 28 February 2025, the Organisation for Economic Cooperation and Development (**OECD**) published a draft framework for the reporting of AI incidents with the aim of providing a global benchmark for key stakeholders. The framework includes 29 criteria to help policymakers understand AI related incidents.

You can read the OECD's announcement [here](#).

**TURKIYE****KVKK PUBLISHES GUIDE TO PROCESSING SPECIAL CATEGORY DATA**

On 26 February 2025, the Turkish Data Protection Authority (**KVKK**) published guidance on the processing of special category data following the



amendment Article 6 of the Law No. 6698 of the Protection of Personal Data which introduces additional conditions for processing special category data.

You can read the KVKK's announcement [here](#) and the guidance [here](#) (only available in Turkish).

## KVKK PROVIDES GUIDELINES FOR SUBMITTING STANDARD CONTRACTS FOR DATA TRANSFERS

On 5 February 2025, the KVKK outlined key requirements for submitting standard contractual clauses to the KVKK, as required by Article 9 of the Law No, 6698. These contracts are considered as a means of ensuring adequate safeguards are in place to transfer personal data to third countries.

You can read the KVKK's announcement [here](#)

---

### CANADA

## OPC PROVIDES UPDATE ON POWERSCHOOL BREACH

On 11 February 2025, the Office of the Privacy Commissioner of Canada (**OPC**) provided an update on the data incident at PowerSchool in January. The OPC's immediate focus is on breach containment, risk mitigation and prevention of future incidents. Affected Canadians have been notified and offered credit monitoring and identity protection services. The OPC announced that it is working closely with the provincial and territorial privacy authorities to ensure the protection of personal data, especially the data of children.

You can read the OPC's announcement [here](#).

## OPC LAUNCHES INVESTIGATION INTO X'S DATA PRACTICES

On 27 February 2025, the OPC launched an investigation into the online platform X following a complaint regarding its data practices. The investigation will investigate whether X is complying with Canada's Personal Information Protection and Electronic Documents Act in relation to its collection, use and disclosure of Canadians' personal data and how it is used to train its AI models.

You can read the OPC's announcement [here](#).

## UNITED STATES OF AMERICA

### TEXAS AG TO INVESTIGATE DEEPSEEK

On 14 February 2025, Texas Attorney General (**AG**) launched an investigation into DeepSeek for allegedly violating the Texas Data Privacy and Security Act. The investigation focuses on its AI platform's privacy practices and calls on Google and Apple to provide information and their analysis

of the DeepSeek app.

You can read the AG's announcement [here](#).

### CALIFORNIA SPONSORS ASSEMBLY BILL 566 ON ONE STEP PRIVACY OPT OUT

On 13 February 2025, California's Privacy Protection Agency (**CPPA**) announced that it has sponsored the Assembly Bill 566 on opt out preference signals, which requires browsers and mobile operating systems to offer consumers a simple one step option to limit the sharing of their personal data through opt out preference signals. The aim of the Bill is to provide consumers with more control over their personal information. If this Bill is passed, California will be the first state to require browsers to support these privacy opt-out signals.

You can read the CPPA's announcement [here](#).

### NEW YORK AG SECURES INJUNCTION TO BLOCK MUSKS' UNAUTHORISED ACCESS TO AMERICANS' PERSONAL DATA

On 21 February 2025, the New York AG has successfully obtained a preliminary injunction from the federal court to stop Elon Musk and his Department of Government Efficiency (**DOGE**) from accessing sensitive Americans' personal information that put citizens at risk. The court's ruling stops DOGE's access to the Treasury's Department's central payment system.

You can read the AG's announcement [here](#).

## FTC ANNOUNCES SETTLEMENT WITH AVAST FOR DECEPTIVE PRIVACY PRACTICES

On 24 February 2025, the Federal Trade Commission (**FTC**) announced that it has settled its claim with Avast following the company misleading its users about its privacy protections. The FTC is sending claim forms to consumers who were affected, and Avast is required to pay \$16.5 million to compensate. The FTC claimed that Avast falsely advertised its software as blocking third party tracking whilst it secretly collected and resold the information processed through browsing data to its subsidiary Jumpshot. Further, the company is prohibited from misrepresenting its data collection practices and from selling browsing data to third parties for the purposes of advertising.

You can read the FTC's announcement [here](#).

## CPPA REACHES SETTLEMENT WITH BACKGROUND ALERT INC FOLLOWING FAILURE TO PAY ANNUAL FEE

On 27 February 2025, the CPPA reached a settlement with Background Alert Inc following its failure to comply with the obligation to register and pay an annual fee to the CPPA under the Delete Act. The company created and sold profiles of individuals through its website using public records. It is now required to stop its operations until 2028 or face a \$50,000 fine.

You can read the CPPA's announcement [here](#).

### BRAZIL

## ANPD IDENTIFIES IRREGULARITIES IN BIOMETRIC IDENTIFICATION SYSTEMS USED BY FOOTBALL CLUBS

On 18 February 2025, the Brazilian National Data Protection Authority (**ANPD**) identified irregularities in the use of facial recognition technology by 23 football clubs during the processing of selling tickets and entry into the stadiums. This concerned transparency obligations, and the legality of processing personal data of children and minors as required by the General Law on the Protection of Personal Data (**LGPD**). The ANPD ordered the clubs to publish information about their use of facial recognition technologies and submit a Data Protection Impact Report within 20 days, explaining the safeguards in place to protect personal data - especially those of young people.

You can read the ANPD's announcement [here](#).

## ANPD TAKES ACTION AGAINST RAIADROGASIL, STIX, AND FEBRAFAR OVER DATA PROTECTION CONCERNS

On 7 February 2025, the ANPD issued preventive measures against Raia Drogasil and Febrafar following an investigation into their handling of personal data, which revealed concerns regarding data protection practices. RaiaDrogasil is required to offer an alternative to providing biometrics, is required to submit information on processing activities to the National Drug Administration and improve transparency information available to customers. The ANPD has also begun an investigation into RaiaDrogasil's use of sensitive information to create behavioural profiles for targeted ads. In addition, the ANPD has required that Febrafar must reevaluate its lawful basis for processing, improve transparency over data use and inform customers regarding their ability to exercise their data protection rights on its website.

You can read the ANPD's announcement [here](#).

## ANPD AND CNIL STRENGTHEN COOPERATION ON AI AND DATA PROTECTION

On 10 February 2025, the ANPD and CNIL announced that they are collaborating to enhance international cooperation on data protection, AI and digital education following the AI Summit that took place in Paris early February. A key focus of the initiative is to ensure the ability to share knowledge and experience between the authorities following the management of AI regulatory sandboxes as well as addressing negotiations on adequacy decision on international data transfers. This collaboration aims to strengthen awareness regarding privacy and data security and advance regulatory strategies in AI.

You can read the ANPD's announcement [here](#).

### SAUDI ARABIA

## SDAIA PUBLISHES DATA TRANSFER RISK ASSESSMENT GUIDELINES

In February 2025, the Saudi Data and Artificial Intelligence Authority (**SDAIA**) published its "Risk Assessment Guideline for Transferring Personal Data Outside the Kingdom", which provides a framework for assessing the risks involved with transferring personal data abroad with foreign entities. The guidelines are split into four phases including preparation, assessing negative impacts, conducting a data transfer risk assessment, and analysing implications for the Kingdom's vital interests. It provides practical steps

for organisations to determine when a risk assessment should be conducted, examine the scope of data processing and to ensure appropriate measures are in place to comply with the Personal Data Protection Law.

You can read the SDAIA's announcement [here](#).

---

## CHINA

### CAC ADOPTS NEW PERSONAL INFORMATION COMPLIANCE AUDIT MEASURES

On 14 February 2025, the Cyberspace Administration of China (**CAC**) implemented new “Personal Information Protection Compliance Audit Management Measures” effective 1 May 2025, which will require organisations to conduct regular audits. The new measure will require organisations to complete an audit at least once every two years for those processing data over 10 million individuals, and for the others, an audit should be conducted frequently based on the level of risk. These audits can be conducted internally or can be outsourced. The new measure specifies the roles and responsibilities of organisations and professional institutions in completing the compliance audits, as well as focusing on areas such as organisational structure, security measures, data incident response procedures and training and awareness programmes. The CAC has also produced an FAQs page on the new measure [here](#).

You can read the CAC's announcement [here](#), and the Order [here](#).

---

### CAC INVESTIGATES AND PENALISES 82 APPS FOR VIOLATING PERSONAL DATA PROTECTION LAW

On 19 February 2025, the Cyberspace Administration of China (**CAC**) investigated 82 apps, including mini programs such as “open a secret room”, following concerns over violations of Personal Information Protection Law. 4 apps were removed following the companies' failure to disclose their collection of personal information and use rules whilst 78 apps were ordered to correct their issues in relation to the ability to delete or correct personal data. The CAC has given these apps one month to comply or face removal.

You can read the CAC's announcement [here](#).



**JAPAN****MINISTRY PUBLISHES CONTRACT CHECKLIST FOR AI USE AND DEVELOPMENT**

On 18 February 2025, Japan's Ministry of Economy, Trade and Industry published a checklist for organisations regarding the contract process when engaging with, developing and using AI models. The checklist has been created to allow businesses to assess the benefits and risks amongst parties and promote safe and lawful use of AI.

You can read the Ministry's announcement [here](#).

**MALAYSIA****PDP PUBLISHES GUIDANCE ON APPOINTING A DPO**

On 26 February 2025, the Malaysian Personal Data Protection Commissioner (**PDP**) published guidelines on the appointment of a Data Protection Officer (**DPO**) guiding organisations on when a DPO should be appointed. The guidelines also outline the roles and responsibilities of the DPO under the Personal Data Protection Act 2010 (Act 709). Organisations are required to notify the PDP within 21 days of appointing a DPO.

You can read the PDP's guidance [here](#) (Only in Malay).

**PDP ISSUES GUIDELINES ON DATA BREACHES FOLLOWING CHANGES IN LAW**

On 26 February 2025, the PDP issued guidelines on data breaches following amendments to the Personal Data Protection Act 2010 Section 12b, which imposes an obligation on data controllers to notify the PDP and the affected data subjects following a data breach that is likely to cause significant harm or is of a significant scale. Organisations are required to report the breach within 72 hours to the PDP.

You can read the PDP's guidance [here](#) (Only in Malay).

**PHILIPPINES****NPC WARNS PUBLIC OVER IRIS SCANNING FOR CRYPTOCURRENCY**

On 20 February 2025, the Philippines' National Privacy Commission (**NPC**) warned the public over reports of

individuals in Bulacan undergoing iris scans in exchange for cryptocurrency. The NPC has emphasised that it does not authorise or approve of the activities that involve the collection of personal information, including biometric data, for such purposes. Under the Data Privacy Act 2012 categories biometric data are sensitive data and its misuse can lead to serious privacy risks. As a result, the NPC urges the public to verify these organisations collecting their data are registered with the NPC and fully understand how they process, store and protect the information collected.

You can read the NPC's announcement [here](#).

## SINGAPORE

### SINGAPORE'S IMDA ISSUES GUIDELINES FOR IMPROVING CLOUD SECURITY

On 25 February 2025, Singapore's Infocomm Media Development Authority (**IMDA**) introduced [new advisory guidelines](#) for cloud services and data centres, aimed at improving the resilience and security of these digital services. The guidelines include best practices within the industry with key measures recommended such as security testing, user access controls, data governance and disaster recovery planning.

You can read IMDA's announcement [here](#).

## SOUTH KOREA

### PIPC SUCCESSFUL IN LAWSUIT AGAINST GOOGLE AND META FOR UNLAWFUL COLLECTION OF USERS' DATA

On 3 February 2025, the South Korean Personal Information Protection Commission (**PIPC**) announced that it won its lawsuit against Google and Meta, following the Seoul Administrative Court decision to uphold the PIPC's sanction against Google and Meta following the companies' unlawful collection of users' data for targeted advertising without obtaining consent. The court found that the businesses failed to adequately inform users and obtain explicit consent, and rejected the companies' argument that consent was obtained via their privacy policies.

You can read the PIPC's announcement [here](#).

## PIPC ANNOUNCES DEEPSEEK SERVICE SUSPENDED IN SOUTH KOREA

On 17 February 2025, the PIPC announced that DeepSeek has temporarily suspended its services in South Korea following concerns raised by the PIPC and its compliance with the Personal Information Protection Act's transparency requirements. The suspension follows the PIPC's request for information into DeepSeek's data protection practices around lawful basis for processing and data storage in China. During the temporary suspension, PIPC will monitor DeepSeek's compliance and assist with aligning its practices with legal requirements.

You can read the PIPC's announcement [here](#).

## PIPC SANCTIONS TWO COMPANIES FOR DATA BREACHES

On 27 February 2025, the PIPC announced that it fined Business on Communication Co Ltd and NHN Wito Co Ltd a total of 198.1 million KRW and an additional charge of 12.3 million KRW for data breaches. Business on Communication Co Ltd was fined 137 Million KRW following a SQL injection attack exposing 179,386 membership records. It was revealed the company failed to implement appropriate security safeguards and delayed reporting the breach to the PIPC. NHN Wito Co Ltd was fined 61.1 million KRW following a cyber-attack which compromised 534,803 customers' data. It was also found that company retained the data for longer than necessary and failed to destroy outdated data. Both companies were issued a corrective order.

You can read the PIPC's announcement [here](#).

**AUSTRALIA****OAIC SIGNS JOINT DECLARATION ON TRUSTWORTHY AI**

On 12 February 2025, the Office of the Australian Information Commissioner (**OAIC**), alongside data protection authorities from South Korea, Ireland, France and the UK, signed a joint declaration aimed at establishing data governance and trustworthy AI. The declaration promotes privacy-by-design principles, ensuring transparency and the need for implementing safeguards through the lifecycle of the AI model.

You can read the OAIC announcement [here](#).

---

**OXFAM AUSTRALIA'S UNDERTAKING ACCEPTED BY OAIC**

On 20 February 2025, the OAIC accepted the EU enforceable undertaking offered by Oxfam Australia following a data breach in 2021, which affected up to 1.7 million records. Although the OAIC has accepted the EU undertaking, this does not confirm that this data breach was a violation of the Australian Privacy Act and the Privacy Principles. However, it shows the importance for charities and not-for-profits to adhere to responsible privacy practices. Oxfam has worked closely with the OAIC and has contributed to an awareness campaign aimed at not-for-profits.

You can read the OAIC announcement [here](#) and the guidance for not-for-profits [here](#).

**OAIC UNVEILS STRATEGY TO DIGITAL ID ENHANCING PRIVACY**

On 26 February 2025, the OAIC announced that it introduced a new Digital ID strategy aimed at improving privacy protections and promoting safer identity verification measures. The Digital ID system offers a secure and voluntary way to verify identity online, without the individual having to provide identity documents multiple times across different organisations. At present, the ID system is available for individuals access government services. However, there is a move to expand this to support identity verification by organisations. The OAIC will enforce strict safeguarding and will act as the privacy regulator for this system.

You can read the OAIC's announcement [here](#).

## NEW ZEALAND

# PRIVACY COMMISSIONER CALLS FOR IMPROVED PRIVACY PRACTICES

On 18 February 2025, the New Zealand Privacy Commissioner (following the outcome of two reports into the protection of personal data including the 2023 Census and COVID-19 vaccination programme) highlighted the need for stronger privacy practices by government agencies. The Commissioner has emphasised the need for personal information to be handled securely and in compliance with the Privacy Act.

You can read the Privacy Commissioner's announcement [here](#).