

### INSIDE THIS ISSUE

#### PG. 4

ICO PUBLISHES  
GUIDANCE ON  
ANONYMISATION AND  
PSEUDONYMISATION

#### PG. 5

COMMISSION  
PUBLISHES THIRD  
DRAFT OF GENERAL-  
PURPOSE AI CODE

#### PG. 24

NEW FEDERAL PRIVACY  
LAW ENACTED IN  
MEXICO



## EU EXTENDS UK ADEQUACY TO DECEMBER 2025 AS THE DUA BILL RAPIDLY PROGRESSES

While the UK's new Data (Use and Access) Bill (**DUA Bill**) is advancing rapidly through Parliament, the European Commission has proposed a welcome extension to the UK's existing adequacy decisions. The proposal would allow the continued free flow of personal data from the EU to the UK until 27 December 2025.

Adequacy decisions allow personal data to move freely from the EU to another country whose data protection laws the EU considers offering an equivalent level of protection. These decisions give EU organisations a straightforward means for transferring data without needing to put additional safeguards in place.

This proposal will help maintain legal certainty for EU-to-UK data transfers while the UK finalises the DUA Bill. When speaking in the House of Commons on 12 March 2025 Minister of State Sir Chris Bryant MP indicated that the Bill is likely to receive Royal Assent by the end of April or early May. If the DUA Bill becomes law, the Commission will be able to reassess whether the UK's updated legal framework offers an adequate level of protection for personal data.

Commissioner for Democracy, Justice, the Rule of Law, and Consumer Protection, Michael McGrath, stated as follows:

*“The adequacy decisions are key to our relationship with the UK. They ensure data can flow freely and safely, which is crucial for trade, justice, and law enforcement cooperation. Our proposal will allow the Commission to assess whether to renew these decisions based on a stable legal framework, while keeping data flows to the UK uninterrupted.”*

Businesses should continue to closely watch this space, as the next few months may bring important developments to UK data protection laws.

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

## UNITED KINGDOM

### UK DATA USE AND ACCESS BILL

In March, the House of Commons concluded its review of the DUA Bill at the committee stage. The DUA Bill is now set to begin the Report stage, however, no date has been scheduled yet.

You can track the progress [here](#) and the Committee Stage Report [here](#).

## OFCOM ENFORCES NEWS OBLIGATIONS FOR PLATFORMS TO TACKLE ILLEGAL CONTENT

On 17 March 2025, the UK’s Office of Communications (**Ofcom**) announced that online platforms are now required to implement appropriate measures to remove illegal content and criminal activity from their platforms. This follows the 16 March 2025 deadline for platforms to conduct an illegal harms risk assessment, as part of Ofcom’s strategy to ensure platforms comply with the Online Safety Act. Ofcom has since launched an [enforcement programme](#) to assess platforms’ compliance and safety measures taken to tackle child sexual abuse material (**CSAM**). Several platforms have been notified that they will be required to provide information on their risk assessments and measures taken to tackle CSAM, with the potential to impose fines for those who fail to do so.

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

## ICO REINFORCES THE RIGHT TO OPT OUT FOR DIRECT MARKETING

On 22 March 2025, the ICO (in connection with the O’Carroll v Meta case) reinforced the right of individuals to object to their personal data being used for direct marketing, including online targeted advertising. Organisations should provide individuals the ability to opt out in a clear and accessible manner. If a company fails to meet an opt out request, those individuals have the right to complain to the ICO. The ICO has announced that it will continue to engage with Meta to ensure their compliance with these regulations.

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

---

## ICO AND CANADA’S OPC ISSUE PROVISIONAL FINE AGAINST 23ANDME FOR DATA BREACH

The ICO and the Canadian Office of the Privacy Commissioner (**OPC**) have been investigating 23andMe following a data breach in 2023. The ICO issued provisional findings, including a notice of intent to fine 23andMe £4.59 million and to issue an enforcement notice. As the company processes sensitive genetic data, additional safeguards are required to meet the standards under the UK GDPR. Although the company has recently filed for bankruptcy in the US, the ICO has made clear that the company is still required to protect its customers under the UK GDPR and will be monitoring the current situation.

You can read the ICO’s statement [here](#).

---

## OFCOM FINES PROVIDER OF ONLYFANS FOR AGE ASSURANCE MEASURES FAILURES

On 27 March 2025, Ofcom imposed a fine of £1.05 million against Fenix International Limited (the provider of OnlyFans) for failing to provide accurate information about its age verification measures. Ofcom previously sought information from the company twice regarding the implementation of age assurance measures and the effectiveness of the third-party facial estimation technology. Fenix had reported that its facial age estimation technology was set at 23, however in 2024 the company discovered it was set at 20. Ofcom found that Fenix failed to meet its duties to provide accurate information within two statutory requests.

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

---

## ADVANCED FINED BY ICO FOR SECURITY FAILURES

On 27 March 2025, the ICO sanctioned Advanced Computer Software Group Ltd £3,076,320 for failing to implement adequate and appropriate security measures leading to a ransomware attack in 2022. The company provided IT services to healthcare providers such as the NHS, without fully deploying multi-factor authentication (**MFA**). Hackers were able to exploit this security gap by entering through unsecure customer accounts into systems. This exposed the personal information of 79,404 individuals, including information on how to get into the homes of 890 people receiving care. This fine, previously at £6.090 million, was reduced following the company's cooperation with the National Cyber Security Centre and National Crime Agency. The ICO emphasised the importance of enabling MFA and implementing appropriate security measures to safeguard personal data.

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

## ICO PUBLISHES GUIDANCE ON ANONYMISATION AND PSEUDONYMISATION

On 28 March 2025, the ICO published its latest guidance on anonymisation, providing organisations practical advice on anonymisation techniques and the advantages and limitations of anonymisation to ensure organisations comply with data protection laws. The guidance:

- Explains the meanings of anonymisation and pseudonymisation
- Outlines data protection obligations and responsibilities
- Provides examples of when data should be anonymised
- Highlights best practices and risk mitigation measures

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

## ICO REVEALS COMMITMENTS TO BOOST ECONOMIC GROWTH

On 17 March 2025, the ICO announced new initiatives it seeks to develop to help businesses use and handle personal data responsibly, with the aim to support the Government's plan to boost economic growth. Key commitments include launching data protection training for small to medium businesses, developing a statutory code of practice for AI, providing simpler guidance for AI, reviewing consent rules within PECR to enable privacy-friendly advertising and updating the guidance on international transfers to help UK businesses access new markets.

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

## EUROPEAN UNION

### EDPB LAUNCHES COORDINATED ENFORCEMENT ACTION ON THE RIGHT OF ERASURE

On 5 March 2025, the European Data Protection Board (**EDPB**) launched its Coordinated Enforcement Framework action for 2025, focusing on the right to erasure (also known as the right to be forgotten) under Article 17 of the GDPR. As a result of the high frequency of erasure requests made and the high volume of complaints concerning handling of the requests, 32 data protection authorities across Europe will be focusing on investigating how organisations process and respond to the right of erasure.

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

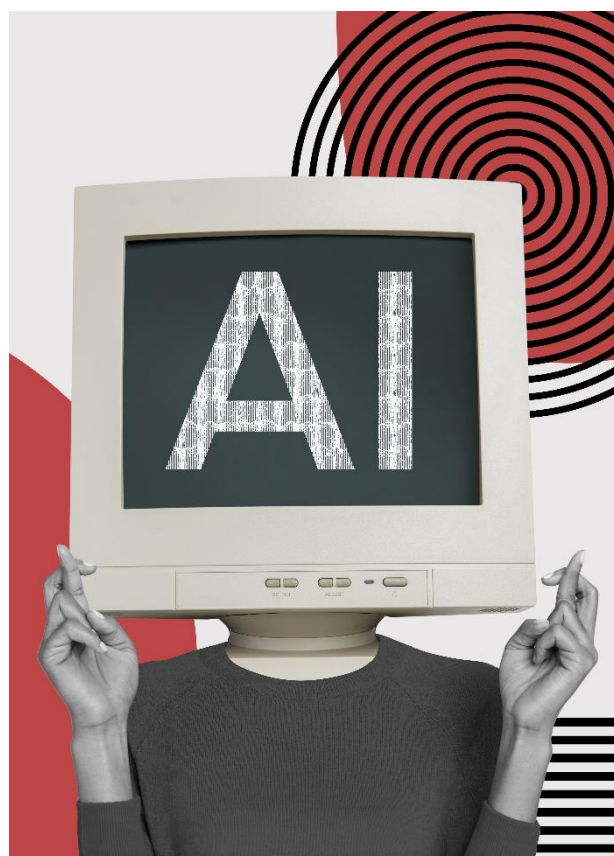
### EU COMMISSION PUBLISHES THIRD DRAFT OF GENERAL-PURPOSE AI CODE

On 11 March 2025, the European Commission published its third draft of the General-Purpose AI Code of Practice after receiving feedback from stakeholders. The Code aims to provide structured “high-level commitments” to transparency, copyright, safety and security for providers of general-purpose AI models that carry systemic risks. The draft Code completed its final consultation at the end of March, aiming to be finalised around [May](#).

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

### COMMISSION IMPLEMENTS RULES ON ESTABLISHING SCIENTIFIC PANEL UNDER THE AI ACT

On 11 March 2025, the European Commission adopted rules to establish a scientific panel under the AI Act, consisting of independent artificial intelligence experts to help support the AI Office.





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

## **CJEU RULING ON CASE REGARDING GENDER IDENTITY IN PUBLIC REGISTERS**

On 13 March 2025, the Court of Justice of the EU (**CJEU**) decided that Hungary must correct the gender identity data in public registers if incorrect, to meet the requirements of the GDPR. An Iranian refugee's asylum records listed the individual as female despite medical certificates confirming the individual as male. The CJEU held that national authorities must meet expectations of rectification due to the absence of gender recognition procedures in national law.

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

## **EDPB RELEASES STATEMENT ON IMPLEMENTING PASSENGER NAME RECORD DIRECTIVE**

On 14 March 2025, the EDPB published a statement on the "[implementation of the Passenger Name Record](#)" following the CJEU on the Passenger Name Record (**PNR**) Directive. PNR includes personal data such as names, travel dates, itineraries, seats, baggage, contact details and payment information provided by passengers and processed by air carriers. The EDPB has provided key recommendations, such as limiting the storage of PNR data to six months unless this can be justified as necessary to the PNR Directive objectives.

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

---

## **COMMISSION ANNOUNCES €1.3 BILLION INVESTMENT FOR IMPROVING AI, CYBERSECURITY AND DIGITAL SKILLS**

On 28 March 2025, the European Commission announced a €1.3 billion investment for the Digital Europe Programme to improve advancements in technology such as AI, cybersecurity, and digital skills. This investment will help support generative AI development and accessibility, support the European Digital Innovation Hubs, and help develop the EU education and training institutions capability.

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

## COMMISSION DISCUSSES POTENTIAL NEW APPROACH TO SIMPLYING GDPR

It was reported that the European Commission plans to propose a simplification of the GDPR to reduce the regulatory and administrative burdens placed on small and medium-sized companies with less than 500 employees. In a livestream on 13 March 2025, the Commissioner for Justice announced the simplification process for the GDPR, stating “a real focus of the European Commission now (is) to improve the competitiveness of the European economy and to bring forward a whole range of simplification measures.” The Commission aims to ease complex requirements such as record keeping obligations for SMEs, whilst preserving the main privacy protection within the GDPR regime. The GDPR will remain a key privacy law. We will monitor developments in this space to provide timely updates.

You can watch the announcement [here](#). (Minutes 3:52 – 5:30)

### AUSTRIA

## DSB ON THE USE OF CAMERAS TO MONITOR WEATHER

On 5 March 2025, the Austrian Data Protection Authority, the DSB, stated that a case-by-case approach should be taken to decide whether the use of cameras for the purposes of recording the weather violates a homeowner’s right to data protection. This followed a complaint from a homeowner in which they were captured by a recording in which the individual was clearly visible. The photographer claimed that the recordings were for the purpose of providing information to tourists about the weather. The DSB decided that the purposes of providing this information could have been achieved without having to record the homeowner and their house.

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

## DSB PRODUCES A CIRCULAR FOLLOWING CJEU RULING ON AUTOMATED CREDIT SCORING

On 25 March 2025, the DSB published a circular following the CJEU’s ruling on Dun & Bradstreet Austria GmbH regarding an automated credit assessment. The circular, informing the Austrian Federal Economic Chambers, aims to raise awareness and provide guidance following the ruling. It details the need for individuals to receive clear, meaningful, and understandable explanations of the automated decision making affecting their personal data.

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

## BELGIUM

### DPA ASKS FOR FEEDBACK ON DIRECT MARKETING RECOMMENDATIONS

On 10 March 2025, Belgium's Data Protection Authority (**DPA**) published its draft recommendations on direct marketing, with a [checklist](#) summarising developments to guide organisations to understand their obligations on direct marketing. The recommendations are open to consultation [here](#) until 10 May 2025.

You can read the DPA's announcement [here](#), and the Recommendations [here](#) (only available in French)

### BELGIUM DATA PROTECTION AUTHORITY REPRIMANDS THE IMMIGRATION OFFICE

On 20 March 2025, Belgium's Data Protection Authority (**DPA**) reprimanded the Immigration Office (**Office**) for unlawfully accessing the prison file of a foreign national residing lawfully in Belgium without a legal basis, and for failing to meet transparency requirements. In 2023, the Immigration Office decided to remove a lawful resident who had committed offences, based on the individual's prison data. Due to the sensitive nature of personal data within the file, it required extra conditions for processing under the GDPR. The DPA found that the Office failed to have a lawful basis for processing the prison file. The DPA reaffirmed the need for appropriate measures to ensure lawful basis is clear. The Office also failed to meet the individual's request for access to their data, and failed to provide transparency information regarding the processing of the individual's data. Therefore, the DPA reprimanded the Office and imposed corrective measures which are to be implemented within 3 months.

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

## BULGARIA

### BULGARIAN COMMISSION, CPDP, INVESTIGATES FACEBOOK PAGE BANNING TEACHERS FROM VARNA

### EDUCATIONAL INSTITUTIONS

On 10 March 2025, the Bulgarian Commission for Personal Data Protection (**CPDP**) announced its investigation into the Varna political party Vazrazhdane's use of Facebook to ban teachers, determining the party did not violate data protection laws in



this case. The teachers had signed a petition opposing amendments to the Preschool and School Education Act. The list included names, workplaces and the subjects that were taught by 26 teachers. It was found that the personal data had come from a public petition which the individuals had consented, meaning disclosure of this information on Facebook was deemed to not breach the GDPR.

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

## CROATIA

# CROATIAN DATA PROTECTION AUTHORITY PROVIDES GUIDANCE FOR CONDUCTING FUNDAMENTAL RIGHTS IMPACT ASSESSMENTS

On 14 March 2025, the Croatian Data Protection Authority, the AZOP, published guidance on the method for conducting a Fundamental Rights Impact Assessment (**FRIA**) as required by the EU AI Act. The FRIA is a mandatory requirement for any AI system likely to be of high risk which should be conducted at the deployment stage. The AZOP recommends that organisations engage with their Data Protection Officer regarding any new projects which aim to use AI, to ensure that the risks are analysed and mitigated as early as possible.

You can read the AZOP's announcement [here](#), and the methodology [here](#) (Only available in Croatian)



## AZOP IMPOSES A TOTAL OF 7 FINES FOR VIOLATIONS TO GDPR

On 24 March 2025, the AZOP imposed fines against seven organisations for violating the GDPR, amounting to a total of €169,000. The largest fine of 80,000 was imposed on a company for unlawfully processing the personal data of individuals, as it collected payment for daily parking tickets. It was found that it had collected the personal data for another purpose and then used that personal data to administer parking fees, as well as failing to have a lawful basis for processing the personal data. In another instance, a €40,000 fine was imposed on a company for publishing personal data online about craftsman without a lawful basis. The company failed to justify the

permanent storage of information of individuals who were no longer listed in the official registers. The other fines were issued for failing to implement adequate security measures and for failing to appoint a data protection officer.

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

---

## CZECH REPUBLIC

### UOOU PUBLISHES PLAN FOR 2025

On 13 March 2025, the Czech Republic's Office for Personal Data Protection, the UOOU, unveiled its plan for 2025 which includes investigating public administrations use of personal data from registers and information systems, obtaining consent from retailers when issuing discounts, the use of camera recording in transport, and sending unsolicited commercial communications.

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

---

### UOOU SIGNS MOU WITH OFFICE FOR THE PROTECTION OF COMPETITION ON AI AND DATA USE

On 14 March 2025, the UOOU announced that it signed a memorandum of understanding with the Czech Office for the Protection of Competition to product workshops and training on business models, AI, and data use.

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

---

## ESTONIA

### ESTONIA'S INSPECTORATE ISSUES STICKERS FOR MISUSE OF CAMERA USE

On 1 April 2025, the Estonian Data Protection Inspectorate (**AKI**) announced that it will distribute stickers on the doors of organisations who have ignored camera usage regulations. The campaign aims to highlight the companies which violate privacy and encourage open discussion on privacy and the balance to be made when using cameras. The stickers will aim to inform the public about hidden cameras, ensuring transparency.

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

## FRANCE

## FRENCH AUTHORITY CNIL PRODUCES DRAFT RECOMMENDATION ON SECURITY OF MEDICAL RECORDS

On 20 March 2025, the French Data Protection Authority, CNIL, published its [draft recommendation](#) for compliance and security of the processing of medical records. Following an increase in data breaches by hospitals, the CNIL produced this recommendation to guide healthcare providers in protecting the personal data they hold. The recommendations include establishing teams determining the sharing of health data between professionals, the use of subcontractors and their obligations, and the implementation of multi-factor authentication and encryption of data. The recommendations are open for public consultation until 16 May 2025.

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

## CNIL ADVISES CUSTOMERS ON RIGHT OF ERASURES AMID 23ANDME UNCERTANTY.

On 28 March 2025, the CNIL provided guidance for customers of 23andMe on how to exercise their right of erasure following the company's filing for bankruptcy and the potential sale of its assets. The company, which provides a genetic testing service, processes highly sensitive information about its customers. Potential risks to customers include sharing of their information with third parties without being informed about what will happen with the information collected following the sale of the company. The CNIL has provided a step-by-step approach for customers to request the deletion of their data, within their statutory rights.

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

## FRENCH COMPETITION AUTHORITY FINES APPLE AND CNIL PROVIDES COMMENTARY

On 28 March 2025, the [French Competition Authority \(ADLC\)](#) imposed a €150 million fine against Apple for "abusing its dominant position in the mobile application distribution sector" when implementing its App Tracking Transparency system. Although the system allows for heightened user privacy by ensuring app providers obtain consent from users, the ADLC found that its implementation was not necessary or proportionate due to constraints imposed on app providers. The decision made by

the ALDC included opinions from the CNIL which called for adjustments to be made to ensure compliance with both GDPR and competition law.

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

---

## GERMANY

### STATE DATA PROTECTION AUTHORITIES REJECT CENTRALISING DATA PROTECTION

On 26 March 2025, the individual German State Data Protection Authorities expressed discontentment with the proposal to centralise data protection supervision. The authorities have argued that the current local structures currently benefit small and medium sized business and freelancers, which make up 99.2% of companies in Germany. The authorities propose reforms to achieve harmonised legal interpretation and simplified procedures without the need for centralisation.

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

---

## GREECE

### GREEK AUTHORITY FINES BANK FOR SECURITY FAILURES

The Greek Data Protection Authority (**DPA**) fined Alpha Bank for a data breach exposing 6,176 employees' information. The breach occurred where an internal employee (who was transferred to another service) retained access to part of a system. It found that the bank failed to remove the employee's role-based access to the system once the employee had moved service, which resulted in loss of confidentiality.

You can read the DPA's announcement [here](#) and the decision [here](#). (Only available in Greek)

### DPA REMINDS ORGANISATIONS OF BREACH NOTIFICATION RESPONSIBILITIES FOLLOWING BREACH AT HELLENIC OPEN UNIVERSITY

On 31 March 2025, the Greek DPA, following a cyberattack at Open University, reminded data controllers of their obligation to notify the affected data subjects if a data breach is likely to pose or poses a high risk to their rights and freedoms.

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

**IRELAND****IRISH COMMISSION, DPC, PRODUCES GUIDANCE ON SUBJECT ACCESS REQUESTS**

On 7 March 2025, the Irish Data Protection Commission (**DPC**) produced a blog post outlining the right of an individual to request access to a copy of their personal data under Article 15 of the GDPR. Organisations can restrict the information provided if a legal exemption applies. The DPC's role includes the ability to investigate complaints made to them regarding the improper handling of data requests and assess whether restrictions were correctly applied. The DPC can also provide advice to organisations on how to manage complex situations.

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

**ITALY****ITALIAN GARANTE FINES GAS COMPANY €300,000**

The Italian Data Protection Authority, the Garante, imposed a €300,000 fine against Energia Pulita srl for making unsolicited marketing calls without obtaining the individual's consent. Around 100 complaints were made to the Garante. It was found that the gas company had used generic forms that failed to provide users to the ability to choose the types of commercial offers, such as telemarketing, they wish to subscribe to. Instead, they used a form that allowed for "omnibus" consent for all types of commercial communication. The Garante's investigation also revealed that the company had used third parties to process the personal data, without meeting the monitoring or training requirements required. The Garante called for the immediate prohibition of any further processing of the unlawfully collected personal data and to implement stricter controls to reduce the risk of entering into sales contracts that would allow for similar violations.

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

**GARANTE FINES TRANSPORT COMPANY FOR UNLAWFULLY EMPLOYEE MONITORING**

The Garante fined a transport company €50,000 for illegally monitoring 50 of its employees through a GPS system installed within company vehicles. The GPS system, (on an ongoing basis) tracked location, speed and vehicle status and failed to comply with data protection laws. The Garante's investigation revealed that the company failed to inform and provide adequate information to its employees and deviated from the

provisions authorised by the Territorial Labour Inspectorate (**Inspectorate**) which required the information to be anonymised. The company was ordered to properly inform employees and align its GPS practices with the Inspectorate's recommendations.

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

---

## DOCTORS FOUND TO HAVE UNLAWFULLY USED PATIENT DATA FOR ELECTORAL CAMPAIGNS

Two doctors were fined €100,000 each by the Garante for their unlawful use of patients' personal data to promote their electoral candidacies, without obtaining free and informed consent. One doctor had contacted around 50 of his patients promoting electoral campaigns. The other was a general practitioner who emailed 500 patients without using blind carbon copying and therefore revealed email addresses and potential health conditions of the patients. Given the highly sensitive nature of health data, the Garante reaffirmed the need for extra care when handling personal data and to only use the information collected for its intended purposes - in this case, to treat their patients and not send out electoral communications.

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

---

### LATVIA

## LATVIAN DATA PROTECTION AUTHORITY PUBLISHES GUIDANCE ON POSTING CLIENT PHOTOGRAPHS

On 5 March 2025, the Latvian Data Protection Authority, DVI, published a guidance blog aimed at professional photographers and their ability to post photos of their clients online. Many professional photographers make use of social media to highlight their work to attract new clients, however the DVI warns that this must be done in line with data protection regulations. Key points for photographers to consider are the legal basis, client expectations, and the need to inform clients about the use of their photographs.

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

---



## DVI COMPLETES PRIVACY NOTICE REVIEW OF 30 ORGANISATIONS

In 2024, the DVI began its investigation into 30 retail organisations' privacy notices published on their websites, compared to the mandatory requirements under Article 13 and 14 of the GDPR. The investigation revealed significant gaps (although not critical) in compliance with these requirements. These included failing to provide contact details of the supervisory authority, use of unclear descriptions of data subject rights and failing to include information on the recipients of personal data. The DVI also noted that in many cases the incorrect lawful basis for processing was used. The DVI recommended organisations use and adapt the template it has provided, as well as making use of the DVI's free resources on preparing a privacy notice.

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

---

## DVI HIGHLIGHTS PROCESSING ACTIVITIES WHICH DO NOT REQUIRE A DPIA

On 6 March 2025, the DVI, following its publication of [guidelines](#) on when a [Data Protection Impact Assessment \(DPIA\)](#) is necessary, provided a list of low risk data processing activities outlining areas which do not require a DPIA. Key areas to note which do not require a DPIA include the processing of employee data handled within Latvia which does not involve biometric, genetic, profiling, or systematic monitoring, and health data which is not transferred to third countries.

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

---

### LUXEMBOURG

## CNPD DECISION UPHELD BY LUXEMBOURG COURT AGAINST AMAZON

On 18 March 2025, the Luxembourg Administrative Court dismissed Amazon's appeal following the Data Protection Authority's (**CNPD**) decision that the company had violated the GDPR, imposing a fine of €746,000. The Court's ruling upholds the fine and corrective measures issued; however, enforcement of these actions has been suspended during the appeal period in case any further proceedings take place.

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

## NETHERLANDS

## DUTCH DATA PROTECTION AUTHORITY OPENS CONSULTATION ON HUMAN OVERSIGHT FOR AUTOMATED DECISION MAKING

On 6 March 2025, the Dutch Data Protection Authority, the AP, opened a consultation on the provision of meaningful human intervention regarding the use of automated decision making, inviting companies, organisations, and experts to contribute. Following the increase in use of algorithms and AI for the purposes of automated decision making and critical decision making, the AP emphasised the importance of organisations to comply with regulations and the right of the individual to have access to human intervention in decisions that could significantly impact them. Human oversight must meaningfully impact the decision-making process and should not just be a symbolic tick box exercise. To help organisations, the AP is developing a tool to help with meaningful intervention, with the hope of providing examples and key questions to help organisations properly implement oversight measures.

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

## AP CRITICISES BILL AIMED AT EXPANDING CODE OF CRIMINAL PROCEDURE LEADING TO EXCESSIVE COLLECTION OF PERSONAL DATA

On 13 March 2025, the AP raised concerns regarding a new bill aimed at expanding the Code of Criminal Procedure to allow police and those with judicial powers the ability to collect large amounts of personal data. The AP acknowledged the need for police to have the resources to investigate, however it warned against the proposal for expanded access, as it lacks adequate safeguards - which can pose risks to individuals and their information caught in police databases. The bill does not adequately regulate how long non-relevant data should be kept and further enables the potential reuse of personal data for purposes beyond the original investigation. The Minister of Justice and Security has announced recently that a committee has been put in place to review data processing in criminal investigations which offers some hope for better safeguards, but the AP insists on the government reviewing this bill to ensure it aligns with data protection requirements before it becomes law.

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

## POLAND

## UODO CONFIRMS CHANGES TO SPORTS PUBLIC DISCLOSURE RULES TO ALIGN WITH GDPR

Poland's President of the Personal Data Protection Office (**UODO**), in January 2025, pointed out concerns about Ordinance No. 19 on public disclosure of personal data by sports associations, stating that the requirement for universal publication of documentation on websites to be transparent interferes with personal data protection rights. As a result, the Minister of Sport and Tourism amended the ordinance in early February 2025 to ensure its compliance with the GDPR. This made changes so the publishing personal data of coaches, instructors, and referees can only be with their consent, limiting the disclosure of membership lists to legal entities, and restricting the publication of management documents to those without sensitive data. These modifications address privacy concerns while maintaining transparency.

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

## UODO ADDRESSES AI REGULATORY CHALLENGES

On 25 March 2025, the UODO announced that it participated in the most recent International Association of Privacy Professionals event, focusing on "Women's Voices in AI: Prospects and Regulatory Challenges for 2025." The President of the UODO emphasised the need to address personal data protection amid the rapid development of AI technologies, and the impact it can have on individuals' rights and freedoms.

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

## META REMOVES COMPLAINT AGAINST UODO

On 24 March 2025, the UODO announced that Meta Platforms Ireland Limited withdrew its complaint against decisions made by UODO, requiring the company to suspend the publishing of false ads on Facebook and Instagram for three months. The ads used deepfake technology to manipulate the images of two individuals, spreading false information, including claims of violent abuse and death. Initially, Meta argued the decisions in court, but later chose to withdraw its complaint, leading to the discontinuation of the legal proceedings.

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

## UODO PRODUCES GUIDANCE ON DPIAS

On 31 March 2025, the UODO produced a guidance blog to help organisations understand when a data protection impact assessment (**DPIA**) should be conducted. UODO reinforces that a DPIA is required where the data processing poses a high risk to individuals' rights and freedoms. Examples include processing of personal data regarding automated decision-making, large-scale processing of sensitive personal data, and systematic monitoring of public spaces. Organisations should leverage the regulatory guidelines to help comply with data protection laws.

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

---

### SLOVENIA

## SLOVENIA'S AUTHORITY PROVIDE UPDATES TO DATA PROTECTION REGULATIONS

On 11 March 2025, the Office for Personal Data Protection of Slovenia (**DPA**) provided an update on the preparation of regulations to address the challenges in personal data protection following changes in technologies advancements, including the rise of cyber threats, artificial intelligence, and recent events. The new regulations aim to simplify the current "double-track regulation" between the European GDPR and Slovenia's law, to ensure alignment with EU and Schengen requirements, and reduce administrative burdens for businesses. Key changes include introducing codes of conduct, harmonising personal data protection laws, reducing administrative burdens for data protection impact assessments and creating a separate law for the transposition of the European Directive on criminal offences.

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

---

### SPAIN

## SPANISH GOVERNMENT PROMOTES PROTECTION OF MINORS

On 25 March 2025, the Spanish Council of Ministers presented a draft bill for the protection of minors in digital environments. The bill aims to address the risks posed by current technological advances and the rise of social media, often leaving minors encountering dangerous and harmful content. Figures show that nearly half of minors with a phone can easily access inappropriate material online. Additionally, a proposed reform to the Personal Data Protection Law aims to replace the age of consent for social media access from 14 to 16 years old.

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

## SWEDEN

### SWEDEN'S NEW CAMERA SURVEILLANCE RULES

From 1 April 2025, organisations in Sweden will no longer need to apply for permission from the Swedish Authority for Privacy Protection (**IMY**) for camera surveillance, but new requirements will be introduced. Public entities, such as municipalities and regions, must now assess if their surveillance complies with regulations before use of camera surveillance. As the new rule enters into force, IMY is increasing its focus on guidance to inform businesses about the new rules. The new regulations will also require organisations to document their plans for camera surveillance and register them, whilst continuing to comply with GDPR and the Camera Surveillance Act for sensitive monitoring.

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

### NOYB TAKES COURT ACTION AGAINST SWEDISH TAX AUTHORITY

On 3 April 2025, Noyb, the European Centre for Digital Rights (a not-for-profit organisation) decided to take the Swedish Tax Authority to court for the authority's use and selling of citizens' personal data to commercial data brokers, who then publish such information online without implementing appropriate data protection measures. The authority is suspected of violating the GDPR. Noyb requires the authority to stop data sharing, arguing it violates the principle of purpose limitation and fails to respect the rights and freedoms of individuals.

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

## ICELAND

### ICELAND'S PERSONUVERND RULES IN FAVOUR OF BANK FOLLOWING PERSONAL DATA HANDLING COMPLAINT

On 6 March 2025, Iceland's Data Protection Authority, Personuvernd, ruled in favour of Arion Bank hf following a complaint from a data subject regarding the processing of their personal data. The complainant raised concerns about being added to the bank's target group list without consent and the bank retaining financial information longer than necessary. The DPA found that the bank's use of the complainant's data for marketing was justified under the bank's legitimate interests, and once the complainant objected, they were removed from the target list.

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

## NORWAY

### NORWAY FINES TELENOR FOR FAILING TO IMPLEMENT AN INDEPENDENT DPO AND INTERNAL GOVERNANCE MEASURES

On 14 March 2025, the Norwegian Data Protection Authority (**Datilsynet**) imposed a fine of 4 million Kroner (approximately £29,480) against Telenor for failing to appoint and implement a data protection officer (**DPO**) and internal governance control measures. The Datilsynet's investigation found that Telenor had failed to properly assess the role of DPO, its independence, failed to provide direct reporting line to top management and had inadequate internal controls. After this decision, the company terminated their DPO, however the Datilsynet has asked them to make an assessment to determine whether a DPO is legally required and, if so, the appropriate measures should be taken.

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

### COMMUNICATIONS AUTHORITY DESIGNATED AS NATIONAL AI COORDINATOR

On 21 March, the Norwegian Communications Authority (**Nkom**) was attributed the role of coordination AI authority, with the aim of allowing the safe and responsible use of AI within Norway. Nkom will work with the Data Protection Authority and other supervisory authorities to strengthen and streamline the governance of AI and ensure compliance with the GPDR and AI regulation.

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

## JERSEY

### JERSEY AUTHORITY IMPOSES £4,000 FINES AGAINST STAR DELTA

On 25 March 2025, the Jersey Office of the Information Commissioner (**JOIC**) imposed a £4,000 fine against Star Delta Electrical Services for posting their client's information onto Facebook. It also found that the company failed to register with the JOIC.

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



## CANADA

## CANADA'S COMMISSIONER SEEKS COURT ORDER AGAINST PORNHUB OPERATOR

On 3 March 2025, the Office of the Privacy Commissioner of Canada (**OPC**) filed an application to the Federal Court seeking an order that would require Pornhub's operator, Aylo, to comply with the privacy laws of Canada. The Federal Court can impose binding orders on companies to comply with the law. The OPC's investigation into Aylo in 2024 found major privacy violations, such as posting highly sensitive and intimate content without the knowledge or consent of the individual.

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

---

## OPC RELEASES DATA BREACH RISK SELF-ASSESSMENT TOOL

On 26 March 2025, the OPC released a new online self-assessment tool to aid organisations to assess whether a data breach poses a real risk of significant harm to individuals. The tool guides users through evaluating the sensitivity of compromised personal data, the likelihood of misuse, and helps determine obligations under the Personal Information Protection and Electronic Documents Act.

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

---

## QUEBEC CAI PUBLISHES OPEN LETTER TO EMPLOYERS ON PROTECTING PRIVACY OF JOB CANDIDATES

On 29 March 2025, Quebec's President of the Commission (**CAI**) signed an open letter calling for employers to protect the privacy of candidates during the recruitment process. This includes the need for establishing an appropriate legal basis, ensuring data minimisation, and implementing safeguards to protect the personal information collected. The CAI has produced guidance on processing candidate information, which can be accessed [here](#).

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

## UNITED STATES OF AMERICA

### NEW YORK ATTORNEY GENERAL ACTS AGAINST ROBOCALLS

On 18 March 2025, the New York Attorney General announced that it has filed an [amicus brief](#) supporting the Federal Communications Commission action to stop telemarketers from collecting phone numbers of consumers and selling them to robocalls without the consumer's consent.

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

### CALIFORNIA ATTORNEY GENERAL ALERTS CONSUMERS OF PRIVACY RIGHTS AMIDST 23ANDME FILING FOR INSOLVENCY

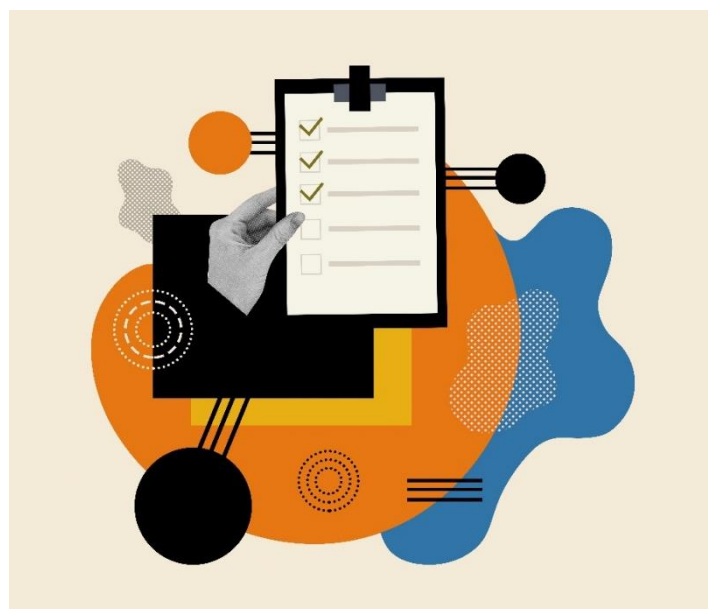
On 21 March 2025, California's Attorney General alerted consumers of 23andMe of their privacy rights, such as the right of deletion under the California Consumer Privacy Act (**CCPA**), following the company's filing for insolvency.

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

### CALIFORNIA ATTORNEY INVESTIGATES SECTOR COLLECTING LOCATION DATA

On 10 March 2025, the California Attorney General announced an investigation into the location data industry, having sent letters to advertising networks, mobile app providers and data brokers suspected of violating the CCPA. Given that many mobile app providers collect the location of their users, concerns have been raised over privacy and the onward sharing of this information with advertising networks and brokers. The investigation will consider whether providers are allowing users to opt out of the sale of their data and the ability to limit the use of their sensitive data, including location data.

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



## VERMONT CONSUMER DATA PRIVACY AND ONLINE SURVEILLANCE BILL PASSES SENATE'S THIRD READING

On 27 March 2025, Vermont's Bill [S.71](#) on "consumer data privacy and online surveillance" passed its third reading in Senate. The Bill was introduced to strengthen data privacy and online surveillance protections for citizens of Vermont, defining key terms, and establishing consumer rights, addressing dark patterns and manipulations of consumer choices.

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

---

## FTC ISSUES LETTER WARNING 23ANDME TO MEET CUSTOMERS' PRIVACY EXPECTATIONS AMID BANKRUPTCY FILING

On 31 March 2025, the Federal Trade Commission (**FTC**) sent a letter to the U.S. Trustees regarding the potential sale or transfer of 23andMe's customers' personal data following the company's filing for bankruptcy. In the letter, the FTC stressed the importance of customers expecting companies to meet their promises of protecting personal data. This includes the customer's right to deletion. The FTC highlighted the importance of 23andMe adhering to promises made within its privacy notice.

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

---

## UTAH PASSES BILL ON CHILD SAFETY WHEN USING SOCIAL MEDIA

In March, Utah's Governor signed a law, the App Store Accountability Act (**Act**), which would require mobile app store providers (such as Apple and Google) to verify the ages of users using their app stores. The Act would put the responsibility of age verification to the providers of app stores rather than individual apps. It will also require parental consent measures are in place for certain apps. The Act is set to enter into force on 7 May 2025.

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

## CPPA FINED HONDA \$632,500 FOR FAILING TO MEET CALIFORNIANS' PRIVACY RIGHTS

On 12 March 2025, the California Privacy Protection Agency (**CPPA**) announced that it fined Honda Motor Co. \$632,500 for breaching the rights of California's residents under the California Consumer Privacy Act. The CPPA's investigation revealed that Honda initiated practices that made it hard for individuals to exercise their rights and prevent their personal data from being shared. It was also found that Honda shared personal data with ad tech companies without implementing proper contractual terms to protect consumers' privacy. Honda has since agreed to implement appropriate measures to ensure Californians can exercise their privacy rights.

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

## NEW YORK GENERAL FINES CAR INSURER \$975,000 FOR DATA BREACH

On 20 March 2025, New York's Attorney General announced that it imposed a \$975,000 fine against a car insurance provider, Root, for failing to safeguard the personal data of 45,000 New Yorkers from unauthorised access. A security gap within the online quote system exposed personal data such as licence numbers, names and dates of birth which were subsequently used by the hackers to file fraudulent unemployment claims. The Attorney General investigation found that the company failed to implement appropriate and reasonable security safeguards to protect the personal data it collected. The company is required to improve its data security by implementing a comprehensive information security program, developing a data inventory, and maintaining authentication procedures.

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

### MEXICO

## NEW FEDERAL PRIVACY LAW ENACTED IN MEXICO

On 20 March 2025, a new Federal Law on the Protection of Personal Data Held by Private Parties was published in the Official Gazette, which entered into effect on 21 March 2025. The new decree updates definitions of key terms such as data controller, processing, personal data, as well as updating requirements of consent, data subject rights and sanctions for violations to the law.

You can read more [here](#) and the law [here](#).

## CHINA

## CHINESE CYBERSPACE ADMINISTRATION INTRODUCES SECURITY MEASURES FOR FACIAL RECOGNITION TECHNOLOGY

On 21 March 2025, the Cyberspace Administration of China (**CAC**) and the Ministry of Public Security announced new security measures for the use of facial recognition technology (**FRT**), which are to take effect 1 June 2025. The measures outline rules and requirements for the processing of biometric facial data, stressing the need for the protection of personal information, the strict adherence to data protection laws and limiting the use of FRT so not to bring about harm to national security, the public interest, and individual rights.

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

## CAC ISSUES MEASURES FOR IDENTIFYING ARTIFICIAL INTELLIGENCE GENERATED CONTENT

On 14 March 2025, the CAC announced new measures for identifying and labelling AI - which are to take effect 1 September 2025. The measures are to promote safe use of AI, its innovation and to protect citizen's rights and freedoms following the increase in use of AI to generate text, pictures, audio, and video. It aims to standardise the identification of AI generated content.

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

## HONG KONG

## PCPD CONCLUDES INVESTIGATION INTO DATA BREACH AFFECTING OVER 100,000 INDIVIDUALS

On 12 March 2025, the Office of the Privacy Commissioner for Personal Data (**PCPD**) of Hong Kong concluded its investigation of a data breach at the Companies Registry and published its findings. The breach (reported in April 2024) originated from the Registry's newly launched system in December 2023, exposing the personal data of individuals due to the setting of the search field which provided additional personal data to searcher's computer. Although the information did not directly appear on the search results page (directing to a web developer tool to be opened) those using robotic searches were able to access the additional information e.g. identify card numbers.

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

---

## PCPD PUBLISHES CHECKLIST GUIDELINES FOR EMPLOYEE USE OF AI AND FINDINGS ON DATA BREACH INCIDENT

On 31 March 2025, the PCPD announced that it published two documents. The first is a checklist on the guidelines for employee use of generative AI, which aims to aid organisations in creating and implementing internal policies around the safe and responsible use of AI by employees in compliance with the Personal Data (Privacy) Ordinance. The second document includes the PCPD's investigation findings of a data breach that occurred at ImagineX Management Company Limited. It found that a hacker exploited a temporary user account, set up for remote support, in which the hacker was able to enter ImagineX's network and access the personal information of over 127,000 people. The PCPD found that the company has failed to implement appropriate security measures and therefore issued an enforcement notice.

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

---

### PHILIPPINES

## PHILIPPINES AND TÜRKIYE SIGN MOU TO STRENGTHEN DATA PRIVACY COLLABORATION

On 11 February 2025, Philippine's National Privacy Commission (**NPC**) and Türkiye's Data Protection Authority, KVKK, signed a Memorandum of Understanding (**MOU**) to improve global data privacy efforts. The MOU aims to enhance collaboration through shared expertise, best practices, and joint research on data protection policies.

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

### SINGAPORE

## SINGAPORE'S UNDERTAKING OF YAMATO TRANSPORT FOR DATA BREACH

On 27 March 2025, the Singaporean Personal Data Protection Commission (**PDPC**) announced that it accepted Yamato Transport's voluntary undertaking to improve its data protection measures following a data breach. In September 2024, Yamato Transport reported a data breach to the PDPC which involved unauthorised access to its server holding clients' and employees' data. Investigations revealed that a threat actor exploited a zero-day vulnerability, executed ransomware, and exfiltrated personal data of 320,482 individuals. The company promptly took



remedial actions, including disconnecting affected servers and patching vulnerabilities.

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

## SOUTH KOREA

### SOUTH KOREA'S DATA PROTECTION AUTHORITY WINS CASE AGAINST META

On 13 March 2025, the South Korean Supreme Court upheld the KRW 6.7 billion fine imposed on Meta by the Personal Information Protection Commission (**PIPC**), as well as the corrective order after finding that Meta did unlawfully share personal data with third parties. In 2020, the PIPC had sanctioned Meta for sharing the personal data of approximately 3.3 million Korean Facebook users to more than 10,000 app operators without obtaining the consent of those users. Meta had then submitted a lawsuit in 2021 challenging this fine, in which the Supreme Court held that the PIPC was correct in its ruling, dismissing the case. The PIPC will now look to ensure that Meta is complying with the corrective order and will monitor the companies' compliance.

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

### PIPC REVIEWS KAKAO'S AI ASSISTANT KANANA

On 13 March 2025, the PIPC announced that it reviewed Kakao's new AI assistant Kanana following Kakao's application for a review of its AI model to ensure privacy by design. The service will leverage Kakao's own large language model, Kanana as well as OpenAI's ChatGPT model, offering users interactive responses within both group and solo settings. Kakao, in an aim to ensure privacy compliance, has consulted with the PIPC and implemented several key safeguards such as encryption of personal data, imposing contractual restrictions on the use of data by OpenAI to only the purposes for which Kakao instructs, and allowing no training to be done by OpenAI on the data. In addition, Kakao will provide users the option to consent before their conversation is used for AI training. An overall risk management system will be put in place to ensure ongoing privacy protections and compliance. The PIPC has approved of these measures and will continue to monitor Kakao's compliance once the AI assistant has been launched.

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

## PIPC SANCTIONS MODUTOUR NETWORK FOR BREACHING OBLIGATIONS UNDER PIPA



On 13 March 2025, the PIPC imposed a KRW 752.2 million fine on Modutour Network Co Lt, a travel agency, for breaching the Personal Information Protection Act (**PIPA**). The PIPC found that the company failed to implement appropriate and adequate security measures which led to a hacker accessing over 3.06 million customers' personal data. The data included names, dates of births, genders and phone numbers of both members and non-members. The company delayed notifying the PIPC about the breach by two months after being made aware, violating the PIPA requirement to notify within 72 hours. It was also found that the company had failed to delete over 3.16 million non-member personal data, which was retained since 2013, increasing the scale of the breach. As a result, the PIPC imposed a total fine of 752.2 million won as well as requesting corrective measures to improve practices.

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

---

## SOUTH KOREA'S GENERATIVE AI USER PROTECTION GUIDELINES ENTER INTO FORCE

On 28 March 2025, the Korean Communications Commission (**KCC**)'s guidelines for safeguarding users from harm when using generative AI entered into force. The guidelines outline four core principles and six implementation methods for developers and service providers to consider.

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

## PIPC FINES WOORI CARD FOR MISUSE OF PERSONAL DATA

On 27 March 2025, the PIPC announced that it fined Woori Card KRW 13.45 billion (approximately \$10 million) for its unlawful use of personal data belonging to 207,000 merchants for marketing without proper consent. Woori was found to have been accessing and sharing information (such as phone number and resident registration numbers) within its sales branches to identify whether the individuals held credit cards with the company. This misuse of data violated the Personal Information Protection Act purpose limitation principles. Following this fine, the PIPC urged companies to regularly review their data processing activities to ensure compliance.

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

### AUSTRALIA

## AUSTRALIA COMMISSIONER URGES GOVERNMENT AGENCIES TO IMPROVE COMPLIANCE

On 19 March 2025, the Office of the Australian Information Commission (**OAIC**) urged government agencies to improve their information governance when using messaging apps, to meet legislative obligations. Following a review of 22 agencies, it found that 16 used messaging apps such as WhatsApp, with only half adopting policies to address such use and compliance with data protection obligations. Most of the policies failed to include key privacy obligations, as well as failing to address Freedom of Information. The OAIC reminded agencies to ensure transparency and accountability.

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