EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

April to June 2023

Executive summary

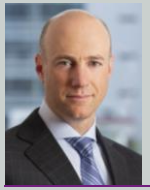
Welcome to the latest edition of Updata!

Updata is an international report produced by Eversheds Sutherland's dedicated Privacy and Cybersecurity team – it provides you with a compilation of key privacy and cybersecurity regulatory and legal developments from the past quarter.

This edition covers April to June 2023 and is full of newsworthy items from our team members around the globe, including:

- Ever-increasing scrutiny and commentary on artificial intelligence (AI) from governments and regulators – including: draft measures in China, a report from the European Union Agency for Cybersecurity, an audit from a German supervisory authority, and rules in New York governing the use of AI in recruitment;
- A flurry of new guidance from the European Data Protection Board (EDPB), including updated guidelines on personal data breach notification, establishment for joint controllers, and on administrative fines;
- A study released by the EDPB on enforcement of GDPR obligations against entities established outside the EEA;
- Progress in the EU legislative adoption procedure for AI regulation, Digital Markets Act and Digital Services Act;
- New practical resources to help businesses navigate supply-chain cybersecurity more easily;
- A white paper released by the UK government surrounding AI, and the Information Commissioner's Office (ICO)'s response;
- A report from Austria showing that there was a 30% increase in cybercrime offences between 2021 and 2022, as well as a report from Sweden that shows 6 out of 10 personal data breaches occur due to human error;
- Following the launch of coordinated action by the EDPB to examine the roles of data protection offices, Sweden has initiated audits against 40 entities;
- A court ruling in Austria that upholds decision to ban use of well-known US web analytics tool due to insufficient safeguards for transfers to the USA, and a similar ruling in Germany;
- A new joint guide for the use of ASEAN model contractual clauses and how they compare against EU standard contractual clauses has been released in Singapore;
- Guidance from the Romanian supervisory authority on the requirements for accreditation of an approved code of conduct under Art. 41 GDPR;
- The UK and USA commit in principle to a "data bridge" to cover adequacy;
- New guidance from Germany surrounding international data transfers post-Schrems II;
- Implementation of whistleblowing protection laws in Bulgaria and Czech Republic;
- New US-state data protection laws in Tennessee, Indiana, Montana and Oregon; and
- Eversheds Sutherland has launched its new 'Metaverse' tool.

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 20 7919 4634
paulabarrett@
eversheds-sutherland.com



Michael Bahar
Co-Lead of Global Cybersecurity and Data Privacy
T: +1 202 383 0882
michaelbahar@
eversheds-sutherland.com

Follow us on Twitter at:

@ESPrivacyLaw

General EU and International

Contributors

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 20 7919 4634
paulabarrett@eversheds-sutherland.com

Theo Davidson
Associate
T: +44 20 7919 4834
theodavidson@eversheds-sutherland.com

Development	Summary	Date	Links
Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR	The EDPB published a study analysing the options available to enforce supervisory authorities' investigative and corrective powers against third country controllers or processors that fall under the scope of Article 3(2) GDPR but are not willing to cooperate and did not designate a representative in the EU or EEA. The study focuses on controllers and processors established in California and in the UK, and also considers how to enforce supervisory powers against controllers and processors established in the People's Republic of China. Among other things, the study found that it is unclear whether supervisory authorities can initiate legal proceedings in another EU Member State or third country on the basis of Article 58(5) GDPR. In addition, the CJEU case law does not confirm whether it the jurisdiction of a Member State would be recognised on the basis of Article 58(5) when the controller/processor has no establishment in that Member State. In addition, the study found that supervisory authorities' may in theory exercise their powers beyond the EEA territories within an international law framework but that this may not always be accepted by the relevant third country. Consequently, the enforcement of EU supervisory authorities' decisions in the courts of California and the UK may prove difficult. However, the third countries' relevant regulatory backdrops (e.g. the California Consumer Privacy Act 2018 and the UK's participation in Treaty 108 as well as its own data protection legislative framework) could open up avenues of co-operation.	13 April 2023	Study

Development	Summary	Date	Links
	The study also identified several "obstacles to international cooperation in the field of data protection" including lack of practice, shortcomings in the legal framework and problems in producing evidence.		
Final guidelines on subject access rights	Following public consultation, the EDPB has adopted a final version of its "Guidelines 01/2022 on data subject rights – Rights of access". In its press release, the EDPB noted that the guidelines provide clarifications on the scope of the rights of access, the information the controller has to provide to the data subject, the format of the access request, the main modalities for providing access, and the notion of manifestly unfounded or excessive requests.	28 March 2023	Guidelines Press release
EDPB clarifies joint controller provisions on in guidelines on identifying lead supervisory authority	The EDPB published updated "Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority". The EDPB had identified that further clarification was required in relation to the concept of main establishment in the context of joint controllership (taking into account its Guidelines 7/2020 on the concept of controller and processor in the GDPR). Section 2.1.3 on joint controllers has been revised to make clear that the concept of a "main establishment" may only apply to single controllers. In a joint controllership arrangement, the main establishment for each relevant controller should be designated on an individual basis.	28 March 2023	Guidelines Press release
Updated guidelines on personal data breach notification	On 28 March 2023, the European Data Protection Board ("**EDPB**") adopted updated Guidelines 9/2022 on personal data breach notification under GDPR. The revised guidelines provide clarity in respect of the **reporting obligations of controllers not established in the EU**. The revisions were made specifically to paragraph 73 and were subject to a consultation towards the end of 2022. The guidelines outline that where a controller not established in the EU is subject to Article 3(2) or Article 3(3) GDPR and experiences a breach, it is still bound by the notification obligations under Articles 33 and 34 GDPR. Article 27 GDPR	28 March 2023	Guidelines Press release

Development	Summary	Date	Links
	requires a controller (and a processor) to designate a representative in the EU where Article 3(2) GDPR applies. In addition, the guidelines now confirm that "the mere presence of a representative in a Member State does not trigger the one-stop-shop system". Consequently, the relevant controller will need to notify the breach to every supervisory authority for which affected data subjects reside in their member state. In its accompanying press release, the EDPB noted that it had decided to publish on its website in the "near future" a contact list for data breach notification with links to accepted languages for all EEA supervisory authorities, in an effort to make breach reporting easier for those controllers not established in the EEA. The guidelines also clarify that it the controller's responsibility to notify the relevant breach, not the representative's.		
Data Protection Guide for small businesses	The European Data Protection Board ("**EDPB**") has launched a Data protection guide for small businesses. The guide contains tools, practical tips and examples in an accessible format to help small businesses understand their data protection compliance obligations. Topics covered include data protection basics, data subject rights and data breaches. The guide is currently available in English but the EDPB plans to publish it in other EU languages.	27 April 2023	Guide
EU AI Act a step closer to becoming law	The Internal Market Committee and the Civil Liberties Committee of the European Parliament have adopted a draft negotiating mandate on the EU's Artificial Intelligence Act ("**AI Act**"), which will be the first EU legislation regulating AI. The AI Act is designed "to ensure that AI systems are overseen by people, are safe, transparent, traceable, non-discriminatory, and environmentally friendly." It follows a risk-based approach, with obligations dependent on the level of risk generated by the AI. This version of the Act incorporates substantial changes to the list of banned AI systems adding onto to the list intrusive and discriminatory uses of AI, for example: remote biometric identification systems used in public spaces; biometric categorisation systems based on sensitive characteristics (e.g. gender, race); predictive policing systems (based on profiling); emotion recognition systems in law	11 May 2023	Press release

Development	Summary	Date	Links
	enforcement, border management, workplace and education, and indiscriminate scraping of biometric data from social media or video surveillance footage to create facial recognition databases. Oher amendments include: – adding further examples of high-risk areas, e.g.: harm to people's health, safety, fundamental rights or the environment, as well as the use of AI systems to influence voters in political campaigns the classification of "high-risk areas to include; – imposing transparency requirements on providers of foundation models (e.g. disclosing that GPT content was generated by AI and preventing the model from generating illegal content); – introducing exemptions from certain rules for research activities and AI components provided under open-source licences. This draft will next need to be endorsed by the European Parliament before negotiations on its final form begin. The vote of the draft AI Act is expected to take place in June.		
Eversheds Sutherland launches guide to the metaverse	Eversheds Sutherland has launched our new legal guide to the metaverse. The metaverse is described by experts as the next iteration of the internet and like the internet will manifest as many different things all at once. For example, the consumer metaverse includes simulated virtual and 3D worlds where people can interact through digital avatars. Its importance is centered around a persistent and immersive shared environment where people can connect regardless of physical location. It is a place where people can buy and sell products and services, learn, be entertained, communicate, exercise and run businesses. Additionally, the industrial metaverse is comprised of virtual worlds where digital twins of cities, transportation systems, airports, factories, grids, and much more mirror their counterparts in the physical world.	May 2023	Guide to the metaverse

Development	Summary	Date	Links
	There is a growing focus on the issues and risks businesses need to be aware of as this technology evolves. In our new guide, Eversheds Sutherland identifies key legal and regulatory challenges which too are evolving as this technology develops. We cover issues in relation to cyber security, data protection, IP, online safety and digital assets. We will be updating our hub over the coming weeks to cover other topics such as managing risks, supply chain management and employment and labor law issues. Explore our guide to the metaverse to discover more. We hope you find it a useful resource.		
EU cyber sanctions regime extended	The EU's regime for imposing restrictive measures against cyber-attacks threatening the EU or its member states has been extended until 18 May 2025.	15 May 2023	Decision
ENISA report on cybersecurity of AI and standardisation	ENISA (the European Union Agency for Cybersecurity) has recently promoted its March 2023 report on cybersecurity of AI and standardisation. The report is intended to set out an overview of cybersecurity standards that are or may be applicable to AI, what they cover and what gaps there are that need to be plugged. Findings include that, because AI is software, existing general purpose technical and organisational standards (eg ISO-IEC 27001 and 9001) can be used in tandem with guidance on how to apply them in an AI context. However, this is not a complete solution: AI can go beyond software to encompass hardware and infrastructure; aspects of cybersecurity are still at R&D stage and are therefore not yet ready to be standardised; and existing standards may not be sufficient to cover all aspects of AI such as traceability and lineage. The report also considers the proposed EU AI Act, emphasising the importance of cybersecurity in carrying out risk assessments, the need for standardised tools and competence for bodies carrying out conformity assessments in order to ensure consistent approach, and the need for the AI Act and the Cybersecurity Act to work together to ensure regulatory coherence.	27 April 2023	Report

Development	Summary	Date	Links
Cyber insurance: a key part of cyber risk planning	The International Association of Insurance Supervisors has published a Global Insurance Market Report special topic edition on cyber. Parts of this report analyse the market for cyber insurance, with key findings including: – there has been a rise in the demand for cyber insurance, driven by a growth in dependence on tech, increased awareness of the "expanding cyber attack surface area" and a sophisticated cyber threat landscape – insurers are imposing stricter conditions, both on obtaining cyber insurance in the first place and on policy scope – cyber insurance is increasingly dealt with by way of a separate policy or endorsement, and can be excluded from all-risk property and casualty policies – there is an indication of a widening of the cyber protection gap, with cyber insurance only covering a small proportion of the potential economic loss that could arise from a cyber event – there is still much uncertainty around cyber catastrophe risk, with the largest cyber event to date being the 2017 NotPetya attack which caused approximately $10 billion in losses, $3 billion of which was covered by insurance These findings are a timely reminder to businesses to consider insurance as part of their cyber risk assessment and mitigation measures. In particular, businesses should look out for cyber exclusions in their general insurance policies, consider whether specific cyber insurance is required, and look carefully at policy terms to assess what types of loss would and wouldn't be covered in the event of a claim.	April 2023	Report
Cybersecurity conversations at board level	The Harvard Business Review has published an article on cybersecurity conversations at board level, focusing on ways in which to increase cybersecurity awareness. This is an important read for all businesses. Key findings include:	2 May 2023	Article

Development	Summary	Date	Links
	– a disconnect between the board and the chief information security officer – a focus on protection from, rather than resilience to, cyberattacks; a cyberattack is a likely occurrence, so businesses need to focus on how they would respond to and deal with the fallout from an attack – cybersecurity needs to be viewed as an "organization and strategic imperative", not a technical topic – insufficient cybersecurity experience amongt board members – if cybersecurity isn't viewed as a priority by the board, this sends the wrong message to the business		
EDPB adopts guidelines for calculating administrative fines	On 24 May the European Data Protection Board (EDPB) adopted guidelines in relation to the calculation of administrative fines under the GDPR. The guidelines, which include an annex containing a summary of the methodology and two illustrative examples, aim to ensure consistency in the approach taken by the data protection authorities. The EDPB makes it clear that the calculation of the amount of fine is still at the discretion of the supervisory authority (subject to the GDPR) and that it should be dependent on all aspects of the case. The methodology provided by the EDPB is a five step process which requires: – identification of the processing operations and the evaluation of the application of Article 83(3) GDPR – the starting point for the calculation of the fines which includes consideration of the number of instances and seriousness of sanctionable conduct possibly resulting in multiple infringements, in addition to the turnover of the business – aggravating and mitigating factors – legal maximums of fines	24 May 2023	Press release Guidelines

Development	Summary	Date	Links
	– an assessment of whether the amount to be find aligns with the requirements of effectiveness, dissuasiveness and proportionality, and if not, to adjust it accordingly. One of the aims of the guidelines is to provide "*harmonisation on the starting points and methodology used to calculate a fine, rather than harmonisation on the outcome.*" It is hoped that through creating this harmonisation, it will also improve efficiencies on cross-border case considerations.		
European Commission consulting on compliance report template for DMA gatekeepers	On 6 June 2023, the European Commission launched a consultation on a draft template for the compliance report that gatekeepers will have to submit under Article 11 of the Digital Markets Act (DMA) regarding contestable and fair markets in the digital sector. Within 6 months of designation, and annually thereafter, each gatekeeper must submit a detailed report which sets out the measures implemented to ensure compliance with those obligations. The draft template is designed to enable gatekeepers to understand the minimum information that must be provided within the compliance reports to allow the European Commission to carry out an assessment of its compliance. This includes: – Information regarding the undertaking of the report, those involved in preparing and drafting the report, and the process of approval. – Details of market testing, expert reports, internal reports and relevant technical data must be provided, as well as details of the undertaking's top 10 business users. Information on compliance with the DMA obligations for each of the undertaking's core platform services including a statement of compliance and explanation on how this has been assessed to show compliance. – Information regarding the gatekeeper's internal compliance and monitoring practices, policies and staff training. The consultation closed on 5 July 2023.	6 June 2023	Consultation

Development	Summary	Date	Links
Good practices for supply chain security	The EU agency for Cyber Security (ENISA) has published its report on Good Practices for Supply Chain Cybersecurity. It brings together the results of an ENISA study last year on investments in cybersecurity budgets among EU organisations, review of the NIS2 directive and gathers good practices. Current practice revealed: whilst supply chain security is recognised the resources devoted to it are lacking, the need for robust governance when making investments and the banking sector leading the way in this area. Good practice focuses on five areas: – a strategic corporate approach is required to supply chain cybersecurity – supply chain risk management using risk assessment processes which then need to be monitored / reviewed. Use of "right of audit" clauses to obtain a clear picture on supply chain practices. – supplier relationship management with reference to ISO/IEC 27002:2022 – vulnerability handling – this ties into supplier management of system vulnerabilities, deployment of patches and keeping abreast of these – is this captured in the contract? – the quality of products and practices for suppliers and service providers – having processes in place which provide quality products as regards cybersecurity…have you agreed testing and assurance procedures? Recommendations to address current challenges include: – aligning terminology so we all operate on a level playing field and have common understanding – thinking about "back door" access / security vulnerabilities in discussions with suppliers – involvement of States when dealing with malicious actors and the importance of sharing information to combat this	13 June 2023	Report

Development	Summary	Date	Links
	– testing and assurance will provide the quality required for products – sharing test platforms across countries To understand more about the impact of the revised proposed Network and Information Security Directive – the EU law which covers this area – read this guide from our EU colleagues. Further afield – our Asia team explain in this briefing the impact of the latest Information Security Technology law in China, and how it will affect those processing data in that country.		
EU Parliament adopts negotiation mandate on AI regulation	A briefing from our AI team summarises the latest developments and consideration on facial recognition in public places being banned as trilogue negotiations between EU Council, Commission and Parliament commence.	14 June 2023	Eversheds Sutherland briefing Press release
Commission consults on transparency requirements of EU DSA	The European Commission has launched a public consultation open until 17 July on the Transparency Database which they have designed for use under the Digital Services Act. Article 24(5) of the DSA prescribes that online providers share their decisions and reasons for removing/restricting content posted by service recipients with the Commission. This is then published on a publicly available and searchable register. The purpose of this consultation is "to give the opportunity to all interested stakeholders and the wider public to provide feedback and suggestions on the precise way this obligation should be implemented, including the information to be collected, the methods for submission of statements of reasons, and the tools of access for the public".	21 June 2023	Press release

Austria

Contributors

Georg Roehsner
Partner
T: +43 15 16 20 160
georg.roehsner@
eversheds-sutherland.at

Manuel Boka
Partner
T: +43 15 16 20 162
manuel.boka@
eversheds-sutherland.at

Michael Roehsner
Legal Director
T: +43 15 16 20 160
michael.roehsner@
eversheds-sutherland.at

Development	Summary	Date	Links
Austrian Constitutional Court to decide on supervision of Data Protection Authority over the Public Prosecutor	The Austrian Constitutional Court will decide on whether the the Data Protection Authority can supervise the Public Prosecutor or whether it violates the Austrian Constitution, given it may be in conflict with the constitutional principle of separation of powers.	9 June 2023	Publication (in German)
Austrian Federal Administrative Court: Sender is not responsible for data processing by postal or logistic service provider	The Court ruled that the sender of a letter is not responsible for unlawful data processing by the postal or logistics service provider, unless this unlawful processing was influenced by the sender. In this case, a letter addressed to a data subject was unlawfully handed over to a third party by the postal service. The Court ruled that this was no violation of data protection law by the sender. A postal service or logistics provider is to be treated as a separate controller rather than a processor of the sender.	Decision: 9 June 2023 Published: 25 May 202	Decision (in German)
Austria presents Cybercrime Report 2022: 30% increase in cybercrime	On 16 May 2023, the Austrian Cybercrime Report 2022 was published. The report shows a 30% increase of cybercrime offences between 2021 and 2022. The Austrian Minister of Interior announced that campaigns have been initiated to improve and speed up police investigations of cyber crimes and to raise awareness in the general population of them.	16 May 2023	Report (in German)
Austrian Federal Administrative Court: legal entities and GDPR	Separately and in addition to GDPR, the Austrian Data Protection Act also provides data protection rights. The Federal	Decision: 16 May 2023	Decision (in German)

Development	Summary	Date	Links
	Administrative Court had previously ruled that this right (based on a constitutional provision) was not repealed by the GDPR. In this new case, the Court now had to decide on the boundaries between GDPR and national data protection legislation. An Austrian legal entity filed a complaint 17 months after discovering the allegedly unlawful processing of their data. The Austrian Data Protection Act limits the period for filing a complaint to one year after discovering the grievance. The complainant argued that this limitation violates the right to lodge a complaint under Article 77 GDPR. The Austrian Federal Administrative Court ruled that, the rights afforded solely under GDPR is limited to natural persons as data subjects. A legal entity's right to data protection is exclusively covered by Austrian national legislation.	Published: 23 June 2023	
Austrian DPA: "Pay or okay" cookie wall of online newspaper requires granular consent – blanket consent violates GDPR	The Austrian Privacy NGO 'noyb' filed a complaint against one of Austria's largest online news portals. The portal uses a "pay or okay" cookie wall. Users can either consent to the data processing (including web tracking) or pay a small monthly subscription fee for ad-free use of the portal. This approach has previously been approved by the Austrian DPA as GDPR compliant. Following this new complaint, the DPA however now ruled that the implementation of the "pay or okay" cookie wall violates GDPR. The DPA confirmed that a "pay or okay" solution can be a basis for a valid consent. However, consent must be granular. This means, data subjects should not only have the choice between no consent or blanket consent for several different processing purposes. Instead, data subjects must have the possibility to consent only to some purposes and not to others. As in this case, no such granular consent was possible, the implementation was deemed not compliant. The decision is not yet legally binding, as an appeal is pending.	7 April 2023	Summary Summary Decision (in German)
Austrian Federal Administrative Court: Use of smart water meters	The Austrian Federal Administrative Court confirmed a ruling by the Austrian DPA on data processing by smart water meters.	Decision: 7 April 2023	Decision (in German)

Development	Summary	Date	Links
by water providers requires customers' GDPR consent	It was decided that data processed by smart water meters about the water usage of an individual household is to be considered personal data. As no other legal basis is applicable, the use of such water meters requires the data subjects' consent.	Published: 2 May 2023	
Austrian Federal Administrative Court: A Social Security Number is not health data under Article 9 GDPR	There has been an ongoing discussion in Austria on whether the Social Security Number of an individual was to be considered health data and therefore special category data under Article 9 GDPR. The Austrian Federal Administrative Court has now confirmed that the Social Security Number by itself is not health data, as by itself it does not provide any relevant information on an individual's health.	Decision: 7 April 2023 Published: 9 May 2023	Decision (in German)
Austrian Federal Administrative Court rules on the use of a dash-cam	The Federal Administrative Court upheld a ruling by the DPA issuing a fine for the use of a dashcam. The Austrian DPA and Austrian Courts have always been very strict regarding the use of dashcams (i.e. cameras in cars, installed to collect evidence in case of an accident). In this new decision, the Court confirmed that a dashcam violates the GDPR if it is constantly active and films the street with a wide-angle lens, even if the data is deleted automatically and accessed only in case of an accident. The use of the camera violated the principles of data minimization, storage limitation and transparency and could not be based on a valid lawful basis. The fine of 250€ issued by the DPA was confirmed.	Decision: 7 April 2023 Published: 2 June 2023	Decision (in German)
Austrian Federal Administrative Court confirms: Use of Web Analytics Tool of US-based service provider violates GDPR	The Austrian DPA was the first EU DPA to decide (in early 2022) that the use of one of the most prevalent Web Analytics tools of a US-based service provider violates GDPR based on the ECJ's "Schrems II" ruling. Since then, several other EU DPAs have issued similar decisions. The Federal Administrative Court has now ruled on one of these decisions by the Austrian DPA and upheld the decision. The Court confirmed the DPA's assessment that analytics data was personal data. It also agreed that the safeguards taken by the analytics service provider when transferring these data to the	Decision: 31st March 2023 Published: 24 May 2023	Decision (in German)

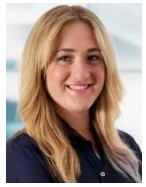
Development	Summary	Date	Links
	USA were not sufficient to comply with Chapter V of the GDPR. The Court reiterated that Chapter V does not allow a "risk-based approach".		

Belgium

Contributors

Koen Devos
Partner
T: +32 2 737 9360
koendevos@
eversheds-sutherland.be

Caroline Schell
Senior Associate
T: +32 2 737 9353
carolineschell@
eversheds-sutherland.be



Stefanie Dams
Associate
T: +32 2 737 9364
stefaniedams@
eversheds-sutherland.be

Development	Summary	Date	Links
Unlawful consultation of camera images	A supermarket in Belgium received a reprimand from the Belgian DPA after conducting customer satisfaction surveys, which involved rating the store's performance. In one particular case, a customer claimed that the (checkout) staff was not always friendly. As a response, the supermarket reviewed the camera footage to verify the claim, but both the employee and the customer appeared to be smiling. The reprimand from the DPA included the following points: – the supermarket had no valid legitimate interest to process the customer's data; – the supermarket did not provide sufficient technical and organizational measures; and – the supermarket had not been transparent enough in its handling of customer data. The DPA concluded that the supermarket's actions were a result of (one-off) human error. However, it emphasized the importance of raising employee awareness and providing proper training on GDPR to prevent similar incidents in the future.	24 May 2023	Decision (in Dutch)

Development	Summary	Date	Links

Complaint concerning refusal of a copy of audio recordings	Telephone conversations were recorded as part of an agreement between a company and a web designer regarding website design services. When the web designer requested a copy of these recordings, the company did not provide it, leading the web designer to file a complaint with the Belgian DPA.
	
	The DPA considered that the company's legal basis for processing the recordings was acceptable, as it was necessary for the execution of the agreement and considered "efficient" in their specific context. Nevertheless, the company was fined a total of EUR 40,000 for the following violations:
	
	– The web designer had the right to receive a copy of the recordings, and a mere transcript or listing of the recordings at the company's office was deemed insufficient. The company could not refuse this right based on reasons such as
	  – privacy of employee;
	  – potential use of the recordings in legal proceedings;
	  – the disclosure of trade secrets in the recordings; or
	  – abuse of rights.
	– Insufficient information was provided in the company's privacy policy. It was unclear which data was collected for what purpose and based on which legal basis. Furthermore, the storage period of the recordings was not clearly defined.
		17 May 2023	Decision (in Dutch)

Bulgaria

Contributors

Irina Tsvetkova
Managing Partner
T: +35 9 2439 0707
irinatsvetkova@
eversheds-sutherland.bg

Victoria Marincheva
Senior Associate
T: +35 9 2439 0707
victoria.marincheva@
eversheds-sutherland.bg

Development	Summary	Date	Links
Ongoing investigation regarding a scheme for collection of data by a voice chatbot	Thousands of people in Bulgaria have received a phone call with an identical script including a female voice which is pretending to ask for delivery feedback by checking if the person resided in the city of Sofia. Representatives of the Bulgarian Commission for Personal Data Protection have expressed an opinion that the mere use of a phone number does not necessarily imply identification of a natural person who is using it.	Decision: 20 June 2023	Decision (in Bulgarian)
Opinion of the Advocate General on the CJEU Case regarding the "hacking attack" against the Bulgarian National Revenue Agency in 2019	In July 2019, the Bulgarian media made it known to the general public that there had been unauthorised access to the information system of the Bulgarian National Revenue Agency ("**NAP**") and that information from its databases containing personal data and tax and social security information had been published on the internet. The total number of natural persons affected, including both Bulgarian and foreign nationals, amounted to 6,074,140. One of the affected data subjects brought an action against NAP for compensation. The Bulgarian Supreme Administrative Court submitted a request to the CJEU for a preliminary ruling regarding issues related to the compensation suffered as a result of the unlawful failure of NAP in its capacity as a data controller, to comply to a sufficient extent with its obligations to ensure appropriate technical and organisational measures under the GDPR. Among the five questions which have been brought before the CJEU, including interpretation of the burden of proof and the scope of the judicial review, the advocate general expressed his opinion on the main issues, namely:	Decision: 27 April 2023	Decision

Development	Summary	Date	Links
	– the fact that the damage was caused by a third party does not in itself constittue a ground for exempting the controller from liability, and, in order to exempt liability, the controller must demonstrate that it is not in any way responsible for the infringement; – the fear of a potential misuse of an individual's data in the future may constitute non-material damage giving right to compensation, provided that the individual demonstrates that he has suffered actual and certain emotional damage to be verified in each individual case..		
The Commission for Personal Data Protection approved standard forms to be used for reporting under the Bulgarian Whistleblowing Act	The Bulgarian Commission for Personal Data Protection ("**CPDP**") approved a standard form for receiving reports under the Law on the Protection of Persons who file Whistleblowers or Publicly Disclose Information on Violations (the "**Whistleblowing Act**"), as well as model records of reports to be kept by the obliged entities. General information on the reporting procedure and instructions how to fill in the report form are provided in the same form. The Whistleblowing Act entered into force on 5 April 2023 and provides that CPDP shall act as a central authority for external submission of reports.	Decision: 20 April 2023	Decision (in Bulgarian)

China

Contributors

Jack Cai
Partner
T: +86 21 61 37 1007
jackcai@
eversheds-sutherland.com

Sam Chen
Of Counsel
T: +86 21 61 37 1004
samchen@
eversheds-sutherland.com

Olivia Chen
Associate
T: +86 21 6137 1071
oliviachen@
eversheds-sutherland.com

Development	Summary	Date	Links
Implementation Rules for the Regulations on the Management of Human Genetic Resources **人类遗传资源管理条例实施细则**	The Ministry of Science and Technology of China ("**MOST**") issued the Implementing Rules on the Administrative Regulations on Human Genetic Resources (the "**Implementing Rules**"). The Implementing Rules clarifies operational questions that have emerged since the Administrative Regulations on Human Genetic Resources ("**HGRs Regulation**") became effective. The Implementing Rules introduces important changes to the previous draft rules made public for comment on March 22, 2022 (the "**Draft Implementing Rules**"). We set forth key points as below: Simplifying the Requirements and Procedure for Disclosure and Sharing of "**HGR data**" – The HGRs Regulation requires a Chinese entity to notify the HGR Administration of China of its disclosure or sharing of any HGR data with a foreign entity. The Implementing Rules specifies that HGR data shall include human genes or genomic data derived from HGR materials, and that clinical data, medical images, protein data and metabolic data, which were previously regulated as HGR data, are excluded from the scope of HGR data.	1 July 2023	Order (in Chinese)

Development	Summary	Date	Links

	– No separate notification is required for the disclosure or sharing of HGR data between a Chinese entity and a foreign entity when the following conditions are met:
	  – prior approval or a recordation filing has been obtained for the Sino– foreign cooperative research project or clinical trial at issue; and
	  – (the parties have agreed by contract to use the HGR data jointly.
	Tightening Control over Data Protection and National Security
	– The Implementing Rules enumerates situations where a security review by the MOST is required for disclosure or sharing of HGR data with a foreign entity such as disclosure or sharing of
	  – HGR data about important genetic pedigrees;
	  – HGR data from specific regions;
	  – exome sequencing and genome sequencing information of more than 500 individuals; and
	  – other cases where China's public health, national security, or social public interests may be impacted
	Clarifying the Scope of "Foreign Entities"
	– The Implementing Rules defines foreign entities as offshore organizations as well as institutions established or actually controlled by offshore organizations or individuals. Control should be deemed to exist where an offshore organization or individual holds more than 50% of the shares, equity, voting rights, or other similar rights and interests, directly or indirectly, in a PRC-domiciled entity.
	Optimizing the Supervision of HGR-Related Activities
	– Under the HGRs Regulation, when applying for advance approval to conduct a Sino–foreign research collaboration utilizing Chinese HGRs, the parties need to provide an ethics review approval obtained in their respective countries/regions. The Implementing Rules allows foreign		

Development	Summary	Date	Links
	entities to use the ethics review opinions obtained by the Chinese partner as a substitute.		
Guidelines for Filing the Standard Contract for Outbound Cross-Border Transfer of Personal Information (First Edition) **个人信息出境标准合同备案指南（第一版）**	The Cyberspace Administration of China ("**CAC**") issued the first edition of guidelines on filing for the standard contract for outbound cross-border transfer of personal information (the "**China SCCs**") (the "**Guidelines**"). The Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information (the "**Measures**") introduces the in detail the route of execution of China SCCs, which is one of the permitted mechanisms for transferring personal information outside of China. The Measures requires the China SCCs to be filed with the CAC and the Guidelines facilitates the implementation of these filing requirements We have noted some key observations below: – Not merely a filing process Based on the Guidelines, the SCC filing process is not purely perfunctory. The CAC retains the discretion to reject an SCC filing. Generally, the controller will be notified of the results of the filing (namely, "passed" or "not passed") from the provincial CAC within fifteen (15) working days from the date of filing. For those who do not pass the filing, the controller will be informed of the reasons for not passing. Where the controller is requested to submit supplemental information to complete the filing, the controller shall resubmit its filing (together with the supplemental information) within ten (10) working days. – The SCCs are "NOT" a loophole to bypass the CAC security assessment requirement: For context, controllers which – process personal data of 1 million individuals or more; – has transferred personal data of 100,000 individuals or more or sensitive personal data of 10,000 individuals or more offshore in aggregate since 1 January of preceding	30 May 2023	Guidelines (in Chinese)

Development	Summary	Date	Links
	year, are required to apply for CAC security assessment in order to transfer data offshore. This process is, by its own nature, very much regulator-led. However, the CAC has observed that some controllers (which processing activities trigger the requirement for a CAC security assessment) may attempt to "split" the total number of data subjects whose personal data are being processed, so that they appear eligible to rely on the SCC route (and are not required to go down the more time-consuming CAC security assessment route). Unsurprisingly, the CAC considers this "splitting" practice unlawful. There are still some uncertainties that arise – for example, the Guidelines have not provided further clarity on the precise meaning of "quantity splitting". In particular, it remains unclear if intra-group, cross-border data transfers will trigger an application on a group level or on a per-entity level. This remains an area of further regulatory clarification. – Uncertainty on Cross-border Transfer remains Unfortunately, uncertainty still exists on the precise meaning of "cross-border transfers" under the PIPL. Specifically, it remains unclear on whether data controllers without operations in Mainland China but processes PRC Data may rely on the SCC regime to transfer PRC Data outside Mainland China. – Required Documents The documents required to be submitted for an SCC filing are substantially similar to those under the CAC security assessment application. Specifically, in addition to the administrative documents provided in the Guidelines (e.g. business incorporation documents), organisations are required to carry out a personal information protection impact assessment ("**PIPIA**") within 3 months before the filing of the SCCs (without major changes as of the filing date), and file the completed PIPIA together with the executed SCCs.		

Development	Summary	Date	Links
	The SCC and the PIPIA should be filed in both physical and electronic form. Further application guidance has been individually released by local CAC branches – as an example, the Beijing CAC and the Shanghai CAC request initial filings to be made electronically through its official email address. We anticipate similar guidance will be issued by other provincial CACs in due course.		
Cybersecurity Standards Practice Guide –Implementation Guidelines for Cyber Data Security Risk Assessment **网络安全标准实践指南一** **网络数据安全风险评估实施指引**	Cybersecurity Standards Practice Guide – Implementation Guidelines for Cyber Data Security Risk Assessment (the "**Implementation Guidelines**") provides ideas, processes, and methods for cyber data security risk assessment and clarifies the steps and content of the assessment. According to the Implementation Guidelines, security risks should be identified and assessed in the context of data security management, data processing activities, data security technologies, and personal information protection. The Implementation Guidelines applies to data processors who conduct security self-assessments, as well as relevant competent authorities who organize inspections and assessments. The appendices of the Implementation Guidelines set out examples of data security risk and a template data security risk assessment report.	26 May 2023	Notice (in Chinese)
Administrative Measures for Generative Artificial Intelligence Services (Draft for Comments) **生成式人工智能服务管理办法（征求意见稿）**	The Draft Measures applies to research, development, and utilisation of generative artificial intelligence ("**Generative AI**") products to provide services to the public within China. Generative AI is defined as technologies that generate text, pictures, sounds, videos, codes, and other content based on algorithms, models, and rules. Before providing any service to the public using a generative AI product, an application for security assessment shall be submitted to the CAC, and a record shall be filed for the algorithm used, amended or cancelled. Generative AI products or services must comply with requirements, including: – in the process of algorithm design, training data selection, model generation and optimisation, and service provision, take measures to prevent discrimination based on race, ethnicity, belief, country, region, gender, age, occupation, etc;	11 April 2023	Notice (in Chinese)

Development	Summary	Date	Links
	– respect intellectual property ("**IP**") rights and business ethics, and not use advantages such as algorithms, data, and platforms to implement unfair competition; – ensure the content generated be true and accurate, and that measures be taken to prevent the generation of false information; and – respect the legitimate interests of others, prevent harm to the physical and mental health of others, damage profile rights, reputation rights, and personal privacy, and IP rights. In addition, the Draft Measures provides that organisations using generative AI must assume the responsibility of the producer for the content generated, and if personal information is involved, assume the responsibility of the personal information processor and fulfil the obligation to protect personal information. Further, the Draft Measures notes that providers are responsible for the legitimacy of pre-training data and training data for generative AI products, and if data contains personal information, providers must obtain the consent of the personal information subject or meet other circumstances stipulated in applicable laws. Likewise, the Draft Measures stipulates that service providers must protect user's input information and usage records, not illegally retain information that can infer the identity of users, and not make profiles based on user input information and usage conditions. Generative AI services must require users to provide real identity information, and establish mechanisms to receive and handle user complaints, and promptly deal with personal information subject requests to correct, delete, and block their personal information. Finally, the Measures states that where corrections of network information departments are refused or the circumstances are serious, the use of generative AI services may be suspended or terminated, and a fine between RMB 10,000 (approx. EURO 1,330) to RMB 100,000 (approx. EURO 13,308) will be imposed.		

Czech Republic

Contributors

Radek Matouš
Partner
T: +420 255 706 554
radek.matous@
eversheds-sutherland.cz

Petra Kratochvílová
Of Counsel
T: +420 255 706 561
petra.kratochvilova@
eversheds-sutherland.cz

Development	Summary	Date	Links
Whistle-blower Protection Act finally adopted and effective from 1 August 2023	The Whistle-blower Protection Act ("**WPA**") applies to reports containing information regarding potential illegal conduct, and its jurisdiction is limited to: – criminal offences; – misdemeanours with a minimum fine of CZK 100,000; – violations of the WPA; and – violations of other legal acts or EU legislation in 14 specific areas. Anonymous reports are not protected by the WPA. Reports should be submitted through the internal reporting system ("**IRS**") in the first place or directly to the Ministry of Justice. The responsible person will evaluate the report and communicate the results to the whistle-blower. Employers with a minimum of 50 employees are obliged to implement an IRS (internally or use some external provider), while small and medium sized employers with up to 249 employees may choose to share an IRS or utilize an IRS operated by another company. Retaliation measures against the whistle-blower or individuals closely associated with them are strictly prohibited; otherwise, they are entitled to adequate compensation and administrative penalties of up to CZK 1 million may be imposed on the employer.	20 June 2023	Legislation (in Czech)

Development	Summary	Date	Links
	The Act will come into effect on August 1, 2023. However, smaller employers with 50-249 employees are not obliged to implement an IRS until December 15, 2023.		
Interim measure to refrain from retaliation against whistle-blowers	The adoption of the Whistle-blower Protection Act (**"WPA"**) led to partial amendments to the Civil Procedure Code. Generally, anonymous whistle-blowers are not covered by the WPA. However, in order to ensure compliance with the WPA, the newly introduced procedural measures will also apply to anonymous whistle-blowers whose identity has been disclosed. One of the instruments to protect whistle-blowers is the interim measure. The court may grant interim measure, in particular, to order the entity named in the report to refrain from any retaliation against the whistle-blower or to pay part of the whistle-blower's remuneration. In addition, the burden of proof will be shifted in disputes arising from retaliation against the whistle-blower. The whistle-blower will only be required to establish the fact of being subject to retaliation (such as dismissal) and assert that it was a result of the report submission.	20 June 2023	Legislation (in Czech)
Draft Methodology on CCTV Systems	The Office for Personal Data Protection ("**OPDP**") launched a public consultation on the draft methodology for the design and operation of closed-circuit television ("**CCTV**") systems with regard to the processing and protection of personal data. The draft methodology on CCTV Systems aims to provide better guidance to controllers and processors of personal data on the obligations relating to the design, installation and operation of CCTV systems. The main purpose of the methodology is to ensure clarity of the obligations under the GDPR and Guidelines 3/2019 on processing of personal data through video devices issued by European Data Protection Board.	28 April 2023	Press Release (in Czech)
Strict liability for unlawful dissemination of commercial communication	The Office for Personal Data Protection ("**OPDP**") imposed a fine of CZK 1.4 million for unlawful dissemination of commercial	6 April 2023	Court Ruling (in Czech)

Development	Summary	Date	Links
	communications promoting goods offered in the company's e-shop. The company argued that it was not responsible for the excesses of its affiliate partners. The Supreme Administrative Court upheld the OPDP's interpretation that liability for the dissemination of commercial communications lies not only with the sender, but also with the person who initiated such dissemination for its benefit. This applies regardless of whether the person did so by using a service or by giving instructions, including the use of affiliate partners or lead marketing tools. The Court emphasised that this liability is strict and that the person who benefits from the dissemination of the commercial communication is also liable for any misconduct of the senders. Therefore, it is important that both the initiator and sender verify the consent of the addressees and comply with the legal requirements.		

Germany

Contributors

Alexander Niethammer
Managing Partner
T: +49 89 54 56 52 45
alexanderniethammer@
eversheds-sutherland.com

Constantin Herfurth
Senior Associate
T: +49 89 54 56 52 95
constantinherfurth@
eversheds-sutherland.com

Christian Dürschmied
Associate
T: +49 30 700140 958
christianduerschmied@
eversheds-sutherland.com

Nils Müller
Partner
T: +49 89 54 56 51 94
nilsmueller@
eversheds-sutherland.com

Isabella Norbu
Associate
T: +49 16 09 36 02 368
isabellanorbu@
eversheds-sutherland.com

Kevin Kurth
Associate
T: +49 89 54565 174
kevinkurth@
eversheds-sutherland.com

Jeanette da Costa Leite
Associate (PSL)
T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

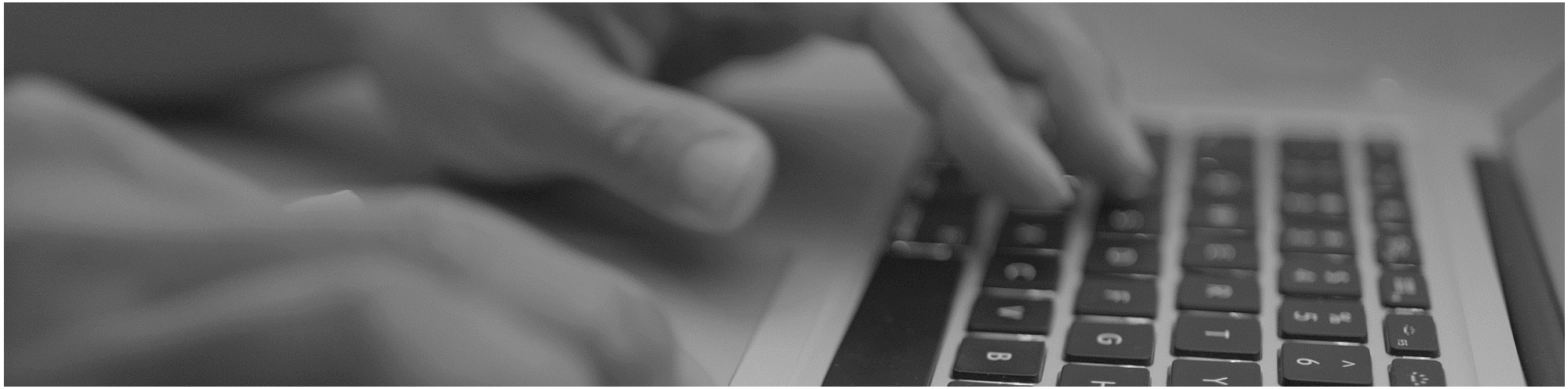
Development	Summary	Date	Links
The data protection officer cannot be the chairperson of the works council at the same time	In its judgement of 6 June 2023, the Federal Labour Court decided that there is typically a conflict of interest between the duties of the chairperson of the works council and the data protection officer ("**DPO**") and that the positions can therefore not be exercised by the same person. Therefore, the DPO can be recalled by the controller on the grounds of Art. 38 (6) sentence 2 GDPR.	6 June 2023	Press release (in German) Court Ruling (in German)

Germany

Development	Summary	Date	Links
New guidelines on international data transfers	The Bavarian State Commissioner for Data Protection has published guidelines on international data transfers. The guidance provides a clear audit scheme and gives an extensive overview on the details of all legal bases for data transfers.	1 May 2023	Guidelines (in German)
New guidelines for GDPR-compliant websites	The Hamburg Commissioner for Data Protection and Freedom of Information has published guidelines on requirements for GDPR-compliant websites. The guidelines examine: – in which cases consent by the data subject is required; – how consent banners should be designed; – how third party content can be integrated; or – what users need to be informed about.	21 April 2023	Guidelines (in German)
Telemarketing cannot be based on Art. 6 (1) (f) GDPR	In its judgement of 20 April 2023, the High Administrative Court Saarland decided that Art. 6 (1) (f) GDPR cannot be used as a justification for marketing calls. Instead, the lawfulness of advertising to data subjects by telephone is based on § 7 of the German Unfair Competition Act (UWG). Therefore, consent of the data subject is generally required for telemarketing.	20 April 2023	Court Ruling (in German)
Audit of ChatGPT	The Supervisory Authority for Schleswig-Holstein sent an official request to OpenAI in order to assess the lawfulness of ChatGPT and GPT to GPT-4 in terms of data protection. The audit was raised by concerns regarding the processing of personal data carried out by the OpenAI products particularlary including: – compliance with data protection principles; – justification by a valid legal basis; and – compliance with information obligations.	19 April 2023	Audit (in German)
New guidelines for updating Records of Processing Activities	The Bavarian State Commissioner for Data Protection has published guidelines on Records of Processing Activities ("**RoPAs**").	1 April 2023	Guidelines (in German)

Development	Summary	Date	Links
	The Commissioner has asked for controllers to regularly update their RoPA and provide detailed advice on the actions required to update the RoPA (e.g. regarding third country transfers or retention periods).		
Judgements on unjustified data subjects access requests	In their judgements of 14 April 2023 and 26 April 2023, the High Regional Court Brandenburg and the District Court Dresden decided that data subject access requests are considered unjustified if they do not aim at assessing the lawfulness of the data processing but, for example, at assessing or preparing civil claims. In such cases, the controller may reject the data subject access request.	1st Ruling: 29 March 2023 2nd Ruling: 26 April 2023	Court Ruling (in German)
Termination of employment without notice in case of multiple data protection violations	In its judgement of 29 March 2023, the District Labour Court Baden-Württemberg decided that the violation of data protection laws can be a reason for dismissal. In the case of multiple violations of the respective provisions by the employee, a dismissal for "good cause" and thus termination without notice can be enforced.	29 March 2023	Court Ruling (in German)
Use of US web-based analytics on websites is unlawful	In its judgement of 23 March 2023, the District Court Cologne decided that the use of the web-based analytics on a website is not justified under the GDPR. If controllers want to implement cookies and transfer the collected data to a third country, they need to rely on: – an adequacy decision; – appropriate safeguards; or – an exemption under Art. 49 GDPR. In particular, there is no such legal basis.	23 March 2023	Court Ruling (in German)
Independent German Federal and State Data Protection Supervisory Authorities decision on pure subscription models for tracking consent	The Independent German Federal and State Data Protection Supervisory Authorities ("**DPSA**") has published a decision on so-called "pure subscription models". This means that the data subject can decide whether he or she wants to give tracking consent when using a website or pay for tracking-free use	22 March 2023	Decision (in German)

Development	Summary	Date	Links
	instead. This fee-based option is important in order to obtain valid consent. The DPSA now decided that pure subscription models are permissible in general, but set certain requirements for website operators. For example, users must be provided with an equivalent service by paying and the fee must be standard market pricing.		



Hong Kong

Contributors

Cedric Lam
Partner
T: +852 2186 3202
cedriclam@
eversheds-sutherland.com

Duncan Watt
Consultant
T: +852 2186 3286
duncanwatt@
eversheds-sutherland.com

Joe Choy
Of Counsel
T: +852 2186 3257
joechoy@
eversheds-sutherland.com

Kelvin Ng
Trainee Solicitor
kelvinng@
eversheds-sutherland.com

Rhys McWhirter
Partner
T: +852 2186 4969
rhysmcwhirter@
eversheds-sutherland.com

Philip Chow
Senior Associate
T: +852 3918 3401
philipchow@
eversheds-sutherland.com

Woody Yim
Legal Manager
T: +852 2186 3298
woodyyim@
eversheds-sutherland.com

Karen Fan
Trainee Solicitor
T: +852 2186 4951
karenfan@
eversheds-sutherland.com

Development	Summary	Date	Links
Privacy Commissioner's Office publishes report on unauthorised access to credit data	The Office of the Privacy Commissioner for Personal Data ("**PCPD**") published an investigation report following a complaint against the operator of a large credit database in Hong Kong. The database offered its services to approximately 680 money lending companies comprising data of about 180,000 borrowers. The Personal Data (Privacy) Ordinance requires that all practicable steps be taken to protect personal data from unauthorised access, processing or use, and to ensure that personal data is not stored longer than necessary. The PCPD	Report on unauthorised access to credit data: 1 May 2023 Announcement of compliance checks: 5 June 2023	Press Release Press Release Report

Development	Summary	Date	Links
	found that the operator had fallen short of the requisite security standards, as it had retained credit records of over 50,000 borrowers and had failed to put in place proper measures to protect personal credit data. Going forward, the PCPD announced that it will proactively conduct compliance checks of all credit reference agencies in Hong Kong. The PCPD recommended measures to credit reference database operators, such as: – adopting personal data privacy management programmes; – imposing heavier penalties to deter recurrence of violations of data protection principles by money lending companies (e.g., increasing the access fees or fines etc.); and – in certain circumstances, consider by terminating their access rights.		
Privacy Commissioner's Office publishes a report on "Privacy Protection in the Digital Age: A Comparison of the Privacy Settings of 10 Online Shopping Platforms"	PCPD published a report examining the privacy settings of 10 popular online shopping platforms Areas examined by the PCPD include the platforms': – privacy policies; – account registration settings; – advertisement / promotional message receipt options; – tracking of users' activities; – transfer of personal data to third parties; – payment options; – readability of privacy policies; and – account deletion options. Among other similarities, the PCPD identified that all investigated platforms had formulated privacy policies, specifying that they collect between 12 to 23 types of personal data, and that all investigated platforms tracked user activities. Findings varied in other aspects, such as how platforms permitted users to indicate	1 June 2023	Press Release Report (in Chinese)

Development	Summary	Date	Links
	the acceptance of promotional messages, and the readability of their privacy policies. The PCPD provided recommendations to the investigated platforms. Among other good practices, operators should only collect necessary personal data and provide users with an option to opt-out of the use of personal data for marketing purposes. They should also provide an easy-to-understand privacy policy and adopt a "Privacy by Default setting". Transparency in tracking users' activities should also be increased, with appropriate options provided for users to decide if they accept such tracking.		
Privacy Commissioner's Office Signs Memorandum of Understanding with its Philippines Counterpart to foster closer collaboration and cooperation in personal data privacy protection	The Philippines' National Privacy Commission ("**PNPC**") and the PCPD executed a Memorandum of Understanding ("**MoU**") on 22 May 2023 to cooperate on data protection matters. In signing the MoU, the PNPC and PCPD will collaborate by sharing information pertaining to cross-border data investigations, breaches and enforcement actions. The two commissions will also collaborate in the training and education of current or emerging data issues. They have agreed to identify suitable organisations to participate in a cross jurisdictional sandbox, which will test-bed innovative data sharing cases. This collaboration indicates the strengthened relationship between the Philippines and Hong Kong in regulatory matters of mutual interest, and represents the growth of both jurisdictions' digital economies while maintaining robust data governance. This may mark the beginning of Hong Kong's increased collaboration with other jurisdictions in terms of data protection frameworks. Organisations should be mindful of such arrangements when handling cross-border data, and should ensure appropriate data privacy compliance protocols are in place.	22 May 2023	Press Release
Privacy Commissioner Publishes Article – "Tech Firms Need to Develop AI Ethically and Responsibly"	Given the growing popularity of generative Artificial Intelligience ("**AI**") -powered chatbots (such as Open AI's ChatGPT), the PCPD published an article with regards to data privacy-related concerns stemming from the use of AI.	17 April 2023	Article Guidance on Ethical Development and Use of Artificial Intelligence

Development	Summary	Date	Links
	Amongst others, the PCPD noted that generative-AI models are trained using massive volumes of unstructured data, which could contain sensitive information. The manner in which sensitive data is collected and used may not be fair nor informed, and may even be susceptible to misuse. Due to AI developers' inclination to keep their data sets proprietary and disclose as little detail as possible, there is a substantial risk that personal data is not collected on an informed basis. Further, AI users may be inadvertently disclosing sensitive information in user conversations, which could be utilised as training data for AI models. As such, the PCPD opined that AI developers should adopt a privacy-by-design approach to mitigate against such risks. This approach involves techniques such as anonymisation to remove all identifiers of data subjects from AI training data, as well as establishing a fair and transparent data collection policy. The PCPD also recommended that reference be made to the principles outlined in its previous publication, the Guidance on the Ethical Development and Use of Artificial Intelligence (published in August 2021).		

Hungary

Contributors

Ágnes Szent-Iványi
Partner
T: +36 13 94 31 21
szent-ivany@
eversheds-sutherland.hu

Kinga Mekler
Senior Associate
T: +36 13 94 31 21
mekler@
eversheds-sutherland.hu

Katalin Varga
Partner
T: +36 13 94 31 21
varga@
eversheds-sutherland.hu

Gréta Zanócz
Associate
T: +36 13 94 31 21
zanocz@
eversheds-sutherland.hu

Development	Summary	Date	Links
National Authority for Data Protection and Information Notice on the obligations of private accommodation providers as data controllers	The National Authority for Data Protection and Freedom of Information (the "**Authority**") has recently received several consultation submissions from individuals providing accommodation services on whether they are covered by GDPR and, if so, what their obligations are. The provisions of the GDPR do not apply to processing for private/household purposes, but since the provider of the accommodation service, regardless of whether he is an individual, is not processing for private purposes but for business purposes, the GDPR applies to the processing carried out during his activities. Consequently, certain processing related to the provision of the accommodation service can only be considered lawful if it is following the provisions of the GDPR. At the time of check-in, the accommodation provider shall record, through the accommodation management software, the identification data of the accommodation user's identity document or travel document, among others. The law defines the purpose of the data processing and provides the legal basis for the processing, as the processing is necessary for the fulfilment of a legal obligation imposed by law on the controller.	31 May 2023	Notice

Development	Summary	Date	Links
	The accommodation provider transmits the data specified in the Act in electronic form and encrypted on a per accommodation basis to the hosting system, i.e., VIZA, using the accommodation management software. The accommodation provider must record the personal data of guests in the accommodation management software at the time of check-in and store them until the last day of the first year after they become known to the accommodation provider. All accommodation providers must have an information on data processing. As personal data relating to the data subject are collected directly from the data subject by accommodation providers, information should be provided to the data subject at the time of obtaining the personal data to ensure fair and transparent processing. In cases where the accommodation provider does not have a website (and therefore, the information cannot be provided to the data subject at the moment of booking) the information on data processing relating to the service should be physically available at the accommodation.		
Retail chain's data processing practices in relation to the purchase of alcoholic beverages	The Authority has received several complaints about the data processing practices of a retail chain in relation to the purchase of alcoholic beverages. According to the complainants, the chains record the date of birth of customers who purchase alcoholic beverages by asking for a photo ID at the checkout, or by requiring them to provide a photo ID, even if they are over 18 years old. The Authority has opened ex officio, a data protection authority procedure in relation to the processing complained about and has carried out two unannounced on-site visits to the controller's shops. The data controller identified the legal basis of a provision of the Consumer Protection Act according to which, before purchasing alcoholic beverages, the business shall, in case of doubt, ask the consumer to provide credible proof of age. The Authority found that the retail chain imposed on its employees, not only in case of doubt, but also as a general rule, a mandatory age verification for	1 February 2023	Order

Development	Summary	Date	Links
	each person intending to purchase alcoholic beverages. It was also established during the procedure that the date of birth recorded by the employees of the controller was not only used by the cash register system to calculate the age of the customer but was also stored as part of the log files for 180 days, to which the data processors of the chain of stores had access. In its decision, the Authority found that the chain's data processing practices breached: – the principles of transparency and data minimisation of the GDPR; – the rules on information to data subjects; the lack of a justified legal basis for the processing; and – the failure to apply appropriate data security measures in the processing. The Authority has ordered the chain to pay a data protection fine of HUF 95 million, to review its age verification practices and to publish an information on data processing on its premises.		

Italy

Contributors

Massimo Maioletti
Partner
T: +39 06 89 32 70 1
massimomaioletti@
eversheds-sutherland.it

Andrea Zincone
Partner
T: +39 02 89 28 71
andreazincone@
eversheds-sutherland.it

Development	Summary	Date	Links
Environmental Agency allowed to continue camera surveillance aimed at major steel producer's site	A major steel producer and 120 of their employees (together: claimants in preliminary relief proceedings) have tried to terminate camera surveillance by the Environmental Agency ("**EA**") on the producer's site by invoking the privacy rights of the employees. The Court found that the camera surveillance does not constitute an invasion of privacy. However, this case is not essentially about privacy law. According to the Court, the case is essentially about something else; namely "the call [..] for more vigorous action against health-damaging emissions of substances into the environment". In this case, the EA had placed a camera outside the producer's site to oversee the emission of harmful substances. The camera was located 450 meters from the production process that the Agency wanted to monitor and continuously records the area around the factory. The video footage that shows black smoke was recorded and retained. The producer considerd this camera surveillance unlawful and demanded its immediate termination. The Court ruled that the producer could not invoke its own right to privacy. After all, the GDPR only protects 'natural persons' and not legal persons. In this case, the Court did not elaborate on whether legal entities are deemed to have privacy rights. The privacy interest of the producer's employees was recognized by the Court. However, the Court also states that there can be no question of a violation of privacy rights under Article 8 of the European Convention on Human Rights if the EA adjusts its work process in such a way that no persons are recognizable in the video footage.	26 April 2023	Court Ruling (in Dutch)

Development	Summary	Date	Links
	Given the configuration of the camera, the Court deemed it highly unlikely that any of the persons appearing on it could be recognized by any official involved in the processing of the material. Nevertheless, the Court did not rule out that the footage could contain traces of the presence of persons present on the producer's site. The Court therefore ruled that, at least in a technical sense, there could be processing of personal data under GDPR. If personal data is involved, a legal basis under GDPR is also required. Pursuant to GDPR, this does not have to be a special category legal basis (Article 9), but the data processing must be able to be classified under one of the listed legal bases of Article 6. In this case, Article 6 paragraph (1) (e) GDPR was relied on: necessity for the performance of a public task, namely the supervision of an environmental permit. The basis includes a proportionality test in the sense of privacy law: processing is only permitted insofar as it is necessary and proportionate for the fulfilment of the public task. In conclusion, the court ruled there was no violation of the principle of proportionality. The camera surveillance could continue.		
The Italian Data Protection Authority fined an apparel company for installing video surveillance systems in violation of applicable employment and data protection law requirements.	The IDPA fined the Italian entity of a multinational group of the apparel sector ("**the company**") for an amount of EURO 50,000, on the account of unlawful deployment of video surveillance systems. The IDPA's investigation began after a trade union reported that video surveillance systems installed by the company in several stores had illegally processed personal data. During the investigation, the IDPA discovered that the company, running a large number of stores in Italy, had not complied with legal requirements for the deployment of systems from which employees' monitoring may derive (i.e., need to reach an agreement with trade unions, or – lacking trade unions or lacking the agreement – need to obtain an authorization from the Italian public labour authorities). The concerned company stated that the installation of the CCTV systems had proved necessary to prevent thefts and to ensure the security of company assets and employees.	Date of IDPA's measure: 26 April 2023 Date of newsletter which made available the measure: 26 May 2023	Decision (in Italian) Newsletter (in Italian)

Development	Summary	Date	Links
	The IDPA's findings showed that all stores had at least three video cameras (up to 27 in larger stores) installed in employees and suppliers areas. These cameras were in operation 24/7, and the images were stored for 24 hours before being overwritten. The IDPA pointed out that the mere posting of information notice in the areas in front of those affected by the shooting is not sufficient to inform data subjects of the presence and operation of the system. The IDPA imposed a fine of EURO 50.000 on the company, taking into account – the significant number of employees involved (more than 500); – the fact that the violation concerned multiple stores; and – the violations of legal requirements for the deployment of systems from which employees' monitoring may derive.		
The Italian Data Protection Authority intervenes on Artificial Intelligence services	The IDPA intervened on the usage of AI services able to simulate and elaborate human conversations, by ordering the provisional suspension of these services and the subsequent restriction of the relevant processing of personal data in Italy on the account of several data protection law violations, including concerning minors, with its measure n. 112 of 30 March 2023. With this measure, the IDPA also prescribed the relevant service provider to communicate within 20 days the adopted measures to comply. After some press releases and approaches among the IDPA officers and AI providers directors, IDPA issued a second measure on 11 April 2023. This second measure revoked the provisional suspension and prescribed several compliance steps in order to make the service fully compliant with data protection laws. On 28 April 2023, the IDPA published a note mentioning the provider's progress and updates and referring to future activities of a European task force on topic.	Date of IDPA's measure: 26 April 2023 Date of newsletter which made available the measure: 11 April 2023	Order (in Italian) Press Release (in Italian) Order (in Italian) Article (in Italian)

Development	Summary	Date	Links
The Italian Data Protection Authority warned two banks that the right to access personal data cannot be restricted for the reason of anti-money laundering in case of publicly available information.	Following investigations triggered by complaints filed by a customer against banks that did not provide a full response to requests for access to personal data, the IDPA stated that, in case of publicly available information, data subjects' right of access to personal data cannot be restricted, since the disclosure of such information does not affect anti-money laundering activities. More specifically, the banks, in accordance with anti-money laundering laws, decided not to provide all the information they had and about which they had become aware through press articles. The news mentioned an investigation against the customer that had ended with a ruling by the Supreme Court. The IDPA found that there was no ground to restrict the right of access in this case, because the data subject's knowledge of such information would have not violated the interests protected by the anti-money laundering laws. In fact, the Supreme Court ruling, as well as press reports, were freely available on the Internet. The IDPA then warned both banks for failing to provide timely and complete responses to the customer's request of access to personal data.	Date of IDPA's measures: 26 April 2023 Date of newsletter which made available the measures: 26 May 2023	Order (in Italian) Order (in Italian) Newsletter (in Italian)
Unlawful telemarketing: new fine to an Italian primary telecommunication operator	The IDPA issued a fine amounting to more than EURO 7.6 million to an Italian primary telecommunications operator for unlawful marketing activities. More specifically, the IDPA found that the operator failed to properly monitor its providers, which included call centres abusively performing marketing calls and that were not part of its official network. In addition, other violations were also contested, such as inadequate response to data subjects' requests to exercise their rights and incorrect publication of personal data in public telephone directories without the consent of the concerned data subjects.	Date of IDPA's measure: 26 April 2023 Date of IDPA's press release: 9 June 2023	Order (in Italian) Press Release (in Italian)

Development	Summary	Date	Links
	In calculating the amount of the fine, the IDPA took both into account the operator's actions to improve data protection compliance.		
Unlawful telemarketing: the Italian Data Protection Authority orders for the first time the confiscation of a call centre database.	The Italian Data Protection Authority ("**IDPA**") fined four companies (respectively, for EURO 200.000, 500.000, 300.000 and 800.000) and ordered, for two of them, the confiscation of their databases used to perform illegal activities. This was the first case in which the IDPA authorized the confiscation of databases of potential customers. The IDPA found these companies responsible of several violations of data protection laws. More specifically, two companies contacted tens of thousands of people using illegally-created lists, without the data subjects' consent for the processing of their data for marketing purposes. These companies proposed commercial offers of energy operators, proposing again after a short time, in order to increase their commissions. Subsequently, contracts concluded through the phone calls were sent to the other two companies for inclusion in the companies' database. The IDPA found that this had been done without any formal assignment and using a fictitious privacy responsibility distribution system, and with serious failures to take effective security measures to protect their systems.	Date of IDPA's measure: 26 April 2023 Date of IDPA's press release: 6 June 2023	Order (in Italian) Press Release (in Italian)
The Italian Data Protection Authority findings on the extent of the right to access personal data in case of denied financing	The IDPA fined a company offering leasing services for an amount of EURO 40.000 for refusing to share information with customers about their creditworthiness that had led to the denial of the requested financing. The complaint was filed by a customer who could not get detailed and related answers to his requests for access to personal data. The customer's goal was to find out the reasons why his application for financing had not been granted. In fact, the company had merely provided the customer with a copy of the documentation he had submitted to apply for financingand invited the data subject to contact a credit rating system (known as "CIS") to receive the requested information.	Date of IDPA's measure: 26 April 2023 Date of IDPA's press release: 22 June 2023	Order (in Italian) Newsletter (in Italian)

Development	Summary	Date	Links
	The IDPA reiterated that the data controller is required to provide all information collected from the CIS and actually used. In addition, the IDPA's investigation revealed that the company rejected the loan application because it had learned of the customer's unreliable credit status after consulting the CIS and, therefore, the controller's partial response prevented the customer from verifying the accuracy of the information processed before deciding on the requested loan. The IDPA fined the leasing company for failing to respond promptly and correctly to the customer's request of access to personal data, reminding that the data controller is required to provide full and up-to-date access to the data subject's data.		

Netherlands

Contributors

Olaf van Haperen
Partner
T: +31 6 1745 6299
olafvanhaperen@
eversheds-sutherland.nl

Judith Vieberink
Senior Associate
T: +31 6 5264 4063
judithvieberink@
eversheds-sutherland.nl

Ilham Ezzamouri
Junior Associate
T: +31 6 3876 4682
ilhamezzamouri@
eversheds-sutherland.com

Robbert Santifort
Senior Associate
T: +31 6 8188 0472
robbertsantifort@
eversheds-sutherland.nl

Frédérique Swart
Junior Associate
T: +31 6 4812 7136
frederiqueswart@
eversheds-sutherland.nl

Nathalie Djojokasiran
Junior Associate
T: +31 6 3820 3704
nathaliedjojokasiran@
eversheds-sutherland.com

Natalia Toeajeva
Junior Associate
T: +31 6 3820 3705
nataliatoeajeva@
eversheds-sutherland.com

Development	Summary	Date	Links
New fines policy for violations under GDPR	The European Data Protection Board ("**EDPB**") published new rules for calculating fines following non-compliance with the GDPR, which have been immediately adopted by the Dutch Data Protection Authority ("**DDPA**") in the Netherlands. Under the new rules, all privacy regulators in the EU will now calculate the fines in the same way. Until now, each privacy regulator in the EU had its own rules. However, by aligning the calculation of fines within the EU, the privacy regulators can ensure that companies are aware of their position and privacy regulators can easily regulate and monitor the organisations.	7 June 2023	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	The new rules, the 'fining guidelines', differ on three important points in comparison to the rules around penalties previously followed by the DDPA, and are as follows: – The company turnover now plays a greater role in calculating the fine amount; – It includes the following three distinct catergories; low, medium and high, which indicate the seriousness of the violation; – the bandwidth to determine starting amount, which can subsequently be increased or decreased; The new fining guidelines will only apply to companies and not government bodies. The government bodies will continue to comply with the fine guidelines within the old DDPA.		
DDPA requests clarification on ChatGPT	The DDPA have raised concerns regarding the handling of personal data by organisations that utilise generative artificial intellgence ("**AI**"), such as ChatGPT. The DDPA intend to take various actions to address these concerns in the near future. Currently, the DDPA have demanded clarification from the software developer, OpenAI, regarding ChatGPT, and among other things, how OpenAI processes the personal data when configuring and training the underlying system, as discussed further below. The DDPA has requested OpenAI to clarify the following: – whether user's questions are used to train the algorithm, and if so, in what way; – the way in which OpenAI collects and uses personal data from the internet; – how information about people is generated by GPT for providing answers to questions; – how generated content that is inaccurate, outdated, inappropriate or offensive can be rectified or deleted.	7 June 2023	DDPA Statement (Dutch only)
Denied data subject's right of access to documents including a	The Court of Appeal has denied an applicant's right of access under GDPR. The applicant in this case was employed by the	23 May 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
request for an opinion by the Dutch District Court	Dutch District Court of Noord-Holland. This case involved incapacity for work and a labour law dispute. The District Court requested the Council for the Judiciary for an opinion on the labour law dispute. The employment contract eventually came to an end after mediation, resulting in a settlement agreement. Subsequently, the applicant requested access to a number of documents under GDPR, including the request for an opinion from the District Court of Noord-Holland to the Council for the Judiciary on the employment dispute. The Court denied this access request, after which the applicant brought proceedings before the Court of Appeal. The applicant argues that the Court did not handle their data subject request in accordance with GDPR. Pursuant to Article 15 GDPR, a data subject may require a controller (in this case the Court) to disclose whether personal data are being processed and if so, to provide access to that data. However, the right of access is limited to personal data. In this case, the data subject access request relates to confidential documents that provide insight into (the creation and content of) the negotiating position of the Dutch District Court in the labour dispute with the applicant. The Court of Appeal concluded that the Court of District had complied with its obligation to provide access since the applicant was provided with the required personal data. In addition, the Court processed this personal data lawfully. Access to confidential documents that provide insight into the formation and content of the negotiating position of the District Court in the labour dispute is not covered by this right of access. The District Court had an important interest in freely and privately determining a position in the employment dispute with the applicant and in preparing the defence against or the initiation of legal action. The denial to the request of access to these documents is therefore proportionate and lawful.		
Fine for bank after inadequate identity check	The DDPA has imposed a fine of 150,000 EUR to a large bank for flawed identity checks by the telephone helpdesk. As a result, clients with a state pension benefit were at risk of having their sensitive data leaked to people who are not entitled to it.	13 April 2023	DDPA Fine (Dutch only)

Development	Summary	Date	Links
	The personal data of a bank's client was leaked to an unauthorised party in 2019. The client discovered that someone had obtained their state pension benefit information via the bank's telephone helpdesk which subsequently lead to a complaint being raised with the DDPA. On average, the bank services over 20,000 customers through their telephone helpline in a week and approximatly 1,500 service employees have access to client data. Therefore, it is vital that the internal guidance for providing personal information via telephone is clear and transparent. The DDPA investigated the bank and identified that the bank's mapping of privacy risks associated with the telephone helpline service was insufficient, for example: – their identity verification system was inadequate, as the control questions asked by the telephone helpdesk to verify the identity of the customers were often on data that could be fairly easily obtained by third parties. – they insufficiently verified whether service employees actually adhered to the inspection policy. – They did not make employees sufficiently aware of the importance of secure management of personal data. The breaches were present betweent the period of May 2018 to May 2022.		
New action plan for improving data exchange in healthcare	The Ministry of Health, Welfare and Sport ("**VWS**") has presented a new Action Plan to improve data exchange in healthcare. The current IT systems are outdated. The plan also focuses on increasing openness, transparency and government direction in order to address the shortcomings in the current healthcare IT landscape.	4 April 2023	Dutch Proposal on data exchange healthcare (Dutch only)
Court ruling on a series of wide-ranging data subject rights; the Court of Appeal in Amsterdam has found in favour of drivers and against taxi operator.	This appeal case was filed by a number of drivers as a result of their accounts being deactivated. The four appellants previously worked as drivers, and utilised the services including the Driver app. Their accounts had been deactivated as the taxi operator suspected that the appellants were guilty of fraud. The District	4 April 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	Court initially dismissed the driver's claims but the drivers appealled the Court's decision. Each of the appellants demanded the following from the taxi operator as part of the appeal: – their accounts to be re-activated; – data subject access request; and – the method of automatic decision making that led to the deactivation of the accounts. Automated Decision Making Method: The appellants requested access to the automated decision-making that took place and led to their accounts being deactivated. This request was declared unfounded by the District Court as they suggested that there was clear human intervention in the decision making process and therefore it was not automated. However, the Court of Appeal took a different approach, and firstly addressedthe right to information in the case of automated decision-making. This is because theremust be a situation in which personal data of the data subjects is used to make a decision without human intervention and there must be a substantial legal consequence associated with this processing. In this case, the substantial legal consequence was the deactivation of the accounts due to the suspicion of fraud. According to the Court of Appeal, the appellants are substantially affected by the deactivation of their account. The drivers could not use the Driver App and as a result, they were at a loss of income. In the first instance, the District Court ruled that the taxi operator should only grant access to personal data related to the rating system used by passengers. The operator refused to disclose any other information requested by the drivers under the pretext of their right to the protection of trade secrets. According to the Court of Appeal, the operator did not demonstrate that a complete refusal is necessary for that protection. The Court ruled that the taxi operator must grant access to the following personal data:		

Development	Summary	Date	Links
	– the profiles of the drivers; – the tags; – individual trip reports; – individual assessments; – upfront pricing system; – information about recipients of personal data; – a category from the guidelines; and – information about automated individual decision-making. With regard to the profiles of the driver, the Court states that the information contained in these profiles must be regarded as personal data in the light of the Nowak judgment of the Court of Justice (EU). The profiles contain information about the communication between the drivers and the operator's customer service. With regard to the reports and individual assessments, the Court concludes that, although the information contained in those reports and individual assessments is relevant to the drivers, the operator was right to anonymise information revealing the identity of the operator's users, as the right of access may not interfere with the right to data protection of other individuals. With regard to information relating to the recipients of personal data, the operator had failed to state the legal basis for non-disclosure, as these restrictions are expressly mentioned in Article 23 GDPR and Article 41 Dutch Implementation Act GDPR. Again, the Court found that the operator also had to provide information about individual automated decision-making, as the data subjects were significantly affected by the decisions and the operator could not demonstrate that human intervention took place. The operator tried to base its non-disclosure on Article 15(4) GDPR, but the Court explicitly stated that this exception only applies to a controller providing copies of processed personal data to data subjects. The operator was also unable to waive disclosure based on trade secret protection, as this argument was		

Development	Summary	Date	Links
	disproportionate to the detrimental impact of the decisions on drivers. The operator must provide drivers with information based on what factors are taken into account, the weight given to those factors by the operator in its ride sharing decisions, fares and average ratings, along with any other information necessary to understand the reasoning behind the decisions.		

Poland

Contributors

Marta Gadomska-Gołąb
Partner
T: +48 22 50 50 732
marta.gadomska-golab@
eversheds-sutherland.pl

Aleksandra Kunkiel-Kryńska
Partner
T: +48 22 50 50 775
aleksandra.kunkiel-krynska@
eversheds-sutherland.pl

Piotr Łada
Senior Associate
T: +48 22 50 50 730
piotr.lada@
eversheds-sutherland.pl

Development	Summary	Date	Links
Government's project in the fight against identity theft	At a recent meeting of the Council of Ministers, the government approved a bill to amend certain laws to reduce some of the effects of identity theft. The purpose of this law is to counter identity theft and protect citizens from its negative effects. According to the provisions of the draft, every citizen will be able to reserve his or her PESEL (Universal Electronic System for Registration of the Population). PESEL number is the national identification number used in Poland which identifies exactly one person and cannot be changed once assigned (among other things, it is used to identify oneself when dealing with authorities, in contracts or for medical services). As a consequence, the Polish Data Protection Authority ("**PDPA**") considered that, in principle, each incident of a breach of personal data processing related to PESEL (e.g. its disclosure in e-mail correspondence) was reportable to the office, but also to the person to whom it belongs, and it affects the assessment of the breach itself, including the amount of the administrative fine. The register of reserved PESEL numbers itself will be maintained by the Minister of Digitisation. It will contain information on reserved and revoked reservations of PESEL numbers, as well as the exact time of their registration (to the nearest second).	16 May 2023	Draft Law (Polish-language version only)

Development	Summary	Date	Links
	The law introduces a catalogue of entities that will be required to verify that a given PESEL number has not been reserved before performing an action. Thus, these entities will not be able to assert claims under the contract if the PESEL number was reserved at the time of its conclusion. The regulations also require telecommunications operators to verify that the PESEL number is not subject to reservation before issuing a duplicate SIM card when entering into a contract with a person for the provision of electronic communication services. This is because the issuance of a duplicate SIM card is associated with serious consequences, such as the possibility of changing the authorisation channel in electronic banking – which would allow fraudsters to take control of assets held at the bank. The bill promises to be an effective tool to prevent the negative consequences of leaking personal data, particularly the PESEL number. From the moment the bill comes into force, administrators, notifying the person whose data has been leaked, will be able to recommend that he or she reserve the PESEL number.		

Portugal

Contributors

Margarida Roda Santos
Partner
T: +35 1 21 35 87 50 0
mrodasantos@
eversheds-sutherland.net

Paulo Sampaio Neves
Lawyer
T: +35 1 21 35 87 50 0
psampaioneves@
eversheds-sutherland.net

Development	Summary	Date	Links
CNPD Opinion 2023/54 on the Draft Law no. 83/XV/1 implementing into national law Directive (EU) 2021/1883 on the conditions of entry and residence of third-country nationals for the purpose of highly qualified employment	To ensure compliance with the GDPR, the PDPA has issued their opinion on the Draft Law no. 83/XV/1, which implements Directive (EU) 2021/1883 on the conditions of entry and residence of third-country nationals for the purpose of highly qualified employment. The PDPA has issued a list of recommendations, including suggestions for clarifying various definitions, purposes of processing personal data and its retention period.	6 June 2023	CNPD Opinion 2023/54 (in Portuguese only)

Romania

Contributors

Mihai Guia
Managing Partner
T: +40 21 31 12 56 1
mihaiguia@
eversheds.ro

Alexandra Sulea
Partner
T: +40 21 311 2561
alexandrahusar@
eversheds.ro

Cristian Lina
Managing Partner
T: +40 21 31 12 56 1
christianlina@
eversheds.ro

Development	Summary	Date	Links
Romanian DPA Decision on approving the Requirements for Accreditation of a Code of Conduct Monitoring Body under Article 41 of Regulation (EU) 2016/679 ("GDPR").	According to the decision by the Romanian DPA, the main requirements for accreditation of an approved code of conduct under Art. 41 GDPR are: 1. **Independence** The monitoring body must demonstrate that it is independent to the members of the code and the profession, industry or sector to which the code applies. If an internal monitoring body is proposed, it must have its own staff, management, responsibility and functions separate from other areas of the organisation. Also, the monitoring body must demonstrate that it is responsible for its decisions and actions in order to be considered independent. Any decision taken by the monitoring body with regard to its functions may not be subject to the approval of the code owner or any other entity. 2. **Conflict of interests** Code owners must demonstrate that the proposed monitoring body will not undertake actions incompatible with its tasks and duties and that safeguards are in place to ensure that it will not undertake incompatible activities. An example of a conflict of interest situation would be where staff carrying out audits or making decisions on behalf of a monitoring	19 June 2023	Link to decision (in Romanian)

Development	Summary	Date	Links
	body have previously worked for the code owner or any of the code organisations. The monitoring body must have its own staff recruited by the body in question or another body independent of the code, and the staff must work exclusively for those bodies. 3. **Expertise** Evidence of level of expertise should include details of the body's knowledge and experience of data protection legislation and the specific sector or processing activity, such as: – ability to indicate previous experience of a monitoring function for a sector; – a thorough understanding of data protection issues and expert knowledge of the specific processing activities covered by the Code; – The staff of the proposed monitoring body must have experience and adequate operational training to ensure the monitoring compliance, such as in the field of auditing, monitoring or quality assurance.		

Singapore

Contributors

Sharon Teo
Partner
T: +65 93 80 2637
sharonteo@
gtlaw-llc.com

Phoebe Sim
Senior Associate
T: +65 66 37 8885
phoebesim@
gtlaw-llc.com

Teo Wen Xuan
Associate
T: +65 66 37 8885
wenxuanteo@
gtlaw-llc.com

Development	Summary	Date	Links
First published PDPC enforcement decision on prohibition under section 48B of PDPA	The Personal Data Protection Commission of Singapore (the "**PDPC**") published its first ever decision on the prohibition on the use of dictionary attacks under section 48B of the Personal Data Protection Act 2012 (the "**PDPA**"). Tai Shin Fatt (the "**Individual**") made a total of 22,268 automated marketing calls ("**Subject Calls**"), of which 433 were to the Singapore Civil Defence Force (the "**SCDF**") emergency line. The Individual authorised his staff to generate, by using a spreadsheet tool, a total of 18,809 telephone numbers ("**Subject Numbers**") to which the automated marketing calls were made. These Subject Numbers included 400 telephone numbers beginning with the digits "995" and consequently, the SCDF emergency line received an influx of marketing calls. The SCDF notified the PDPC, which proceeded to commence investigations to determine whether the circumstances relating to the calls disclosed any breaches of the PDPA. The PDPC held in its decision that: – The Individual was in breach of section 48B of the PDPA due to the method used in generating the telephone numbers in	17 April 2023	PDPC's decision

Development	Summary	Date	Links
	question and the Individual's role in authorising the marketing calls. – A dictionary attack was carried out in this case. As per section 48A of the PDPA, "**dictionary attack**" means "the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations". – By using a dictionary attack to generate the Subject Numbers and then causing and/or authorising the Subject Calls to the Subject Numbers, the Individual failed to stay within the clear guardrails of the PDPA to safeguard consumer interests. Organisations should note that when sending unsolicited commercial messages, special care must be taken to avoid indiscriminate ways in which recipient telephone numbers can be generated and targeted by automated means, in addition to observance of the Do Not Call provisions under the PDPA.		
MAS Consultation Paper on "Enhancing Safeguards for Proper Conduct of Digital Prospecting and Marketing Activities"	The Monetary Authority of Singapore ("**MAS**") published a consultation paper that sets out proposals to enhance safeguards for proper conduct of digital prospecting and marketing activities. In relation to data protection, MAS proposes to refine the requirements in FAA-N02, to strengthen financial institutions ("**FIs**")' oversight and control of activities conducted by lead generation firms and enhance safeguards for proper handling of customers' data. In this regard, MAS has proposed amendments to FAA-N02, to require FIs to monitor activities and conduct of lead generation firms. As customers' data must be handled with proper care, the proposed amendments also require FIs to ensure that the manner in which lead generation firms collect, use or disclose data, is in line with the FI's own data management policies and applicable laws such as the PDPA. Further, MAS is considering providing a transition period of six to nine months for FIs to comply with the new Guidelines, updated Regulations and Notice, i.e. the effective date of these	25 April 2023	MAS Consultation Paper Current Notice 'FAA-N02'

Development	Summary	Date	Links
	instruments would be six to nine months from their issuance date.		
Regulatory Framework for Artificial Intelligence Governance in Singapore	The Ministry of Communications and Information (the "**MCI**") is planning to issue advisory guidelines on the use of Personal Data in AI Systems under the PDPA by the end of 2023. Where necessary and useful, the MCI will update measures to take into account the impact of AI developments such as ChatGPT and GPT-4.	9 May 2023	MCI response to Parliament question
Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses	The Joint Guide to ASEAN Model Contractual Clauses ("**MCCs**") and EU Standard Contractual Clauses ("**SCCs**") was launched at the Computers, Privacy & Data Protection Conference in Brussels on 24 May 2023. The MCCs and SCCs are model data protection clauses ("**clauses**") that can be incorporated by parties (e.g. data exporters and importers) in their contracts as a basis to allow the transfer of personal data across borders. The incorporation of the clauses is on a voluntary basis. The clauses act as a tool to ensure that personal data continues to benefit from a high level of protection in cases of international transfers and, in particular, to ensure compliance with applicable legal requirements for international data transfers in this regard. The Joint Guide provides a comparison between the MCCs and SCCs. Companies already familiar with the MCCs may consider using the Joint Guide as a reference point for their contractual negotiations on data transfers with their EU business partners.	24 May 2023	PDPC's announcement
Launch of AI Verify Foundation to Shape the Future of AI Standards Through Collaboration	The AI Verify Foundation was set up by the Singapore Infocomm Media Development Authority to harness the collective power and contributions of the global open-source community to develop AI testing tools for the responsible use of AI. The AI Verify Foundation will seek to improve AI testing capabilities and assurance to meet the needs of companies and regulators globally.	7 June 2023	Press release
Joint Press Release on the accession of the Republic of Korea	On 8 June 2023, the Republic of Korea acceded to the Digital Economy Partnership Agreement ("**DEPA**"), making it the first	9 June 2023	Press release

Development	Summary	Date	Links
to the Digital Economy Partnership Agreement	partner outside of the founding members, Chile, New Zealand and Singapore, to join. The DEPA is an agreement which set outs approaches and collaborations in digital trade issues, promotes interoperability between various regimes and addresses the new issues brought by digitalisation.		
Memorandum of Understanding for Cooperation in the Field of Cybersecurity	On 21 June 2023, the Cyber Security Agency of Singapore and the National Cyber Security Agency of Qatar signed a Memorandum of Understanding ("**MOU**") for Cooperation in the Field of Cybersecurity. The MOU will strengthen Singapore and Qatar's ability to address and tackle the transboundary challenge of cybersecurity by: – Facilitating information sharing between both countries' Computer Emergency Response Teams, and facilitating exchanges to better secure Industrial Control Systems and Operating Technology used in Critical Information Infrastructure systems; – Collaborating on mutual areas of national interest; and – Setting out further areas of potential cooperation, such as research, cybersecurity education and training, and partnership on national initiatives of mutual interest.	22 June 2023	Press release

Slovakia

Contributors

Jana Sapáková
Counsel
T: +421 232 786 411
jana.sapakova@
eversheds-sutherland.sk

Daša Derevjaniková
Associate
T: +421 232 786 411
dasa.derevjanikova@
eversheds-sutherland.sk

Development	Summary	Date	Links
Report of Slovak Data Protection Authority for the year 2022	The Office for Personal Data Protection of the Slovak Republic ("**the Office**") submitted its report on the state of personal data protection for the year 2022 to the National Council of the Slovak Republic. The 2022 report is an overview of the Office's activities in the period under review, which shows, among other things: – 120 personal data breaches were formally reported to the Office, of which up to 102 were relevant; – the three most frequent breaches of the GDPR found in 2022 were: – breach of the principle of lawfulness, fairness and transparency under Article 5(1)(a) of the GDPR (73%); – violation of the principle of accountability under Article 5(2) of the GDPR (62%); and – breach of the information obligation under Article 13 of the GDPR (51%).	26 April 2023	Report of Slovak Data Protection Authority for the year 2022 (only in Slovak)
New guidlines on processing CCTV data installed in homes	In 2022, a large portion of the Office's activities involved responding to instances consisting of the processing of personal data by CCTV installed in homes. Therefore, on 24th May 2023, the Office issued a new guideline under No 1/2023 on this matter. The Office stated that there may be a legitimate interest of the owner/occupier of the family home to process the personal data of a third person by monitoring the area around the house. However, the Office pointed out that the owner/occupier of the	24 May 2023	Guideline (only in Slovak)

Development	Summary	Date	Links
	home has several data protection obligations which arise from this – including the development of a proportionality test. In conclusion, the Office advised to use CCTV in such a way as to ensure that footage is only captured within the boundaries of the property. By doing so, the risk of complaints from the persons concerned and possible control or action by the Office can be minimized.		
The Slovak Republic has ratified CETS Protocol 223	On 15th June 2023, the Slovak Republic ratified the CETS 223 Protocol amending the Council of Europe Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (ETS 108). It became the 25th country to approve the Protocol.	15 June 2023	Ratification of the CETS Protocol 223

South Africa

Contributors

Grant Williams
Partner
T: +27 10 003 1375
grantwilliams@
eversheds-sutherland.co.za

Matthew Anley
Senior Associate
T: +27 10 003 1382
matthewanley@
eversheds-sutherland.co.za

Development	Summary	Date	Links
Information Regulator requests Private Bodies to submit annual reports for the 2022/23 financial year on access to information requests received and processed	Pursuant to section 32 of the Promotion of Access to Information (PAIA), the Information Officer of every Public Body is obliged to submit an Annual Report to the Information Regulator detailing access to information requests received and processed by the Public Body during the previous year. While there is no statutory obligation on Private Bodies to submit such an Annual Report, the Information Regulator may, in terms of section 83(4) of PAIA, request Private Bodies to furnish it with reports about requests for access to records of the Private Body. During May 2023, the Information Regulator issued an invite to all Public Bodies and Private Bodies to submit their Annual Reports on access to information requests received and processed during the 2022/23 financial year, to the Information Regulator, by 30 June 2023. The Annual Reports can be submitted through the portal created by the Information Regulator. To assist Public Bodies and Private Bodies with the submission of their Annual Reports, the Information Regulator has published a Manual for PAIA Section 32 Reports, which is available on its website. According to the Information Regulator: – the objective of the submissions is to determine whether Public Bodies and Private Bodies are receiving and recording requests for information. – the data from the reports will provide a picture of the status of compliance with PAIA and its implementation in Public Bodies and Private Bodies.	Invitation to submit the Annual Report for 2022/23 financial year: 31 May 2023 Deadline for submission of Annual Reports for 2022/23 financial year: 30 June 2023	Invitation to submit the Annual Report for 2022/23 financial year, in respect of access to information requests received & processed by Public and Private Bodies, in terms section 32 and section 83(4) of PAIA Information Regulator media statement Manual for PAIA Section 32 Report Information Regulator Portal webpage

Development	Summary	Date	Links
	– the report will also help to ascertain the usage of PAIA by members of the public when it comes to access to information, and help measure or indicate the levels of awareness of PAIA from the side of the requester, and Public Bodies and Private Bodies.		

Sweden

Contributors

Torbjörn Lindmark
Partner
T: +46 8 54 53 22 27
torbojnlindmark@
eversheds-sutherland.se

Sina Amini
Associate
T: +46 72 451 25 34
sinaamini@
eversheds-sutherland.se

Development	Summary	Date	Links
Administrative fine of SEK 200,000 issued against a Swedish region due to a missing USB flash drive containing sensitive data	The Swedish Authority for Privacy Protection (the "Swedish DPA") has issued an administrative fine of SEK 200,000 against a Swedish region. A personal data breach was reported to the Swedish DPA after an employee of the region had lost an unencrypted USB flash drive that contained social security numbers and other sensitive personal data relating to over 2,000 data subjects. The main reason behind the administrative fine was that the region had not encrypted the USB flash drive. Therefore, the region had failed to implement sufficient organisational and technical measures in relation to the sensitivity of the personal data that was being processed.	27 April 2023	Press statement (in Swedish) Decision (in Swedish)
Supervisory plan for 2023 now published by the Swedish DPA	The supervisory plan for 2023 has now been published by the Swedish DPA. The Swedish DPA will continue to primarily focus on investigating complaints from data subjects. Additional focus areas include camera surveillance in public areas and the role of the data protection officer. In regard to audits taken by the Swedish DPA's own initiative, the plan is to follow a risk-based approach. Priority is based on a set of criteria, where at least two of them of the following criteria needs to be fulfilled: – a serious violation, or risk, of the individual's right to privacy; – if the processing affects or may have consequences for a large number of data subjects;	15 May 2023	Press statement (in Swedish) Supervisory plan for 2023 (in Swedish)

Development	Summary	Date	Links
	– new technology that may substantially affect the individual's right to privacy; – a substantial need for guidance; or – a serious breach of good practice in debt collection or illegal debt collection or credit reporting activities.		
A municipality has been prohibited from using CCTV in certain public areas	Pursuant to the Swedish Camera Surveillance Act (2018:1200), using CCTV to monitor public areas generally requires a permit from the Swedish DPA. A municipality had for more than one year used CCTV to monitor certain public areas without applying for a permit. The municipality argued that a permit was not necessary as the monitoring was anonymised through the use of pixelation technology. The Swedish DPA concluded, however, that by recording CCTV footage and then transferring said footage to a server for the purpose of removing the identity of individuals captured by the CCTV through pixelation technology, constitutes by itself a form of data processing pursuant to GDPR. For this reason, a permit to use CCTV was required pursuant to national law and the municipality was prohibited from using CCTV in those areas without said permit.	15 May 2023	Press statement (in Swedish) Decision (in Swedish)
6 out of 10 personal data breaches occur due to human error, according to report published by the Swedish DPA	The Swedish DPA has published a report on data breaches that were investigated during 2022. The report concludes that 6 out of 10 personal data breaches occur due to human error and that the actual number of incidents may be three times as many compared to the number of incidents reported to the Swedish DPA. In particular entities in the private sector are reporting less incidents compared to previous years. Accidentally sending an e-mail or letter to the wrong person or address continues to be the most commonly reported personal data breach. The report further compares reported personal data breaches with other Nordic countries and concludes that Denmark has had	7 June 2023	Press statement (in Swedish) Report (in Swedish)

Development	Summary	Date	Links
	the most reported incidents for 2022, followed by Finland and then Sweden. The same ranking also applies when calculating the number of reported incidents per 100,000 citizens.		
Swedish DPA will focus on initiating more audits based on complaints from data subjects	Back in March 2023, the European Data Protection Board (EDPB) launched a coordinated action to examine the role and position of data protection officers (DPO). The coordinated action involves 26 European data protection authorities, including the Swedish DPA. The Swedish DPA has now initiated audits against approximately 40 entities, including businesses within the financial and insurance sector as well as certain public authorities and municipalities. The audit will include answering a number of questions relating to DPOs, for example whether the organisation's management has clearly defined and prepared a written description of the DPO's tasks, what tasks the DPO has and whether the DPO has sufficient resources to perform these tasks. The Swedish DPA also wants to find out whether the DPO's advice is generally followed by the organisation and whether the organisation documents cases where they decide not to follow it.	12 June 2023	Press statement (in Swedish)
Known music streaming service issued an administrative fine of SEK 58 million	A known music streaming service has been issued an administrative fine of SEK 58 million due to providing insufficient or unclear information to data subjects who had requested access to the personal data which the company processed about them. Most of the investigation relates to matters between November 2021 to May 2022. The Swedish DPA concluded that the information which the company provided upon request by a data subject was too general and that it needed to be adapted to the specific recipient. For instance, it was pointed out that the information regarding transfers to countries outside the EEA did not specify whether the data subject's personal data was subject to such data transfers even though the information was provided pursuant to Article 15 GDPR (right to access). Information regarding the purposes for processing, third party recipients and sources were presented to the data subject in relation to several categories of personal data. The problem was,	13 June 2023	Press statement (in English) Decision (in Swedish)

Development	Summary	Date	Links
	however, that some categories such as 'user data' did not further specify exactly what personal data was being processed by the company. According to the Swedish DPA, the lack of clarity meant that the data subject would not be able to understand the provided information which constituted a breach of GDPR. Another issue was regarding complex information such as technical data or metadata. The Swedish DPA found that in certain cases it was insufficient to only have the information available in English and that the company was required, if necessary, to provide an explanation in the data subject's native language. The company argued that technical data (e.g. log data) dynamically changed over time and a translation would thus be necessary several times a month. Additionally, the company deemed it would be unreasonable and disproportionate to be required to provide translations for all local languages, in particular considering that many technical terms only had an official wording in English. It was noted, however, that the company has stated that they have the possibility upon request by the data subject to translate the description of the data in the technical log files into a local language to the extent that the technical terms are translatable. Since a translation is therefore possible in practice, it was concluded that such a translation should be provided even before a request for translation has been made by a data subject. The company's stated difficulty in translating the data, including the fact that translation may need to be done several times each month and the additional resources this would require, cannot justify that the information is by default provided in English. In regard to the size of the administrative fine, it should be noted that this was the first time that the Swedish DPA applied European Data Protection Board (EDPB)'s guidance on the calculation of administrative fines under GDPR. The final version of the guidance was adopted by EDPB on 7 June 2023.		
Administrative fine of SEK 13 million issued against a media group due to incorrect profiling	A media group has been issued an administrative fine of SEK 13 million by the Swedish DPA due to profiling customers and website visitors without a valid legal basis pursuant to GDPR.	27 June 2023	Press statement (in Swedish) Decision (in Swedish)

Development	Summary	Date	Links
	The media group had collected personal data about customers and website visitors from several sources across different group companies for the purpose of providing targeted advertisement to these data subjects. The collected data included historical purchases made in various group companies and website behaviour that had, in some cases, been combined with other personal data from other sources such as information about the data subject's gender, car ownership and mailing address. The media group had relied on their legitimate interest to provide advertisement, however, the Swedish DPA considers that customers and other website visitors cannot reasonably expect to have information about how they use a website and other collected data be used for targeted advertisement without their express consent. The type of profiling conducted by the media group would require consent as a legal basis pursuant to GDPR.		Link

United Kingdom

Contributors

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 20 7919 4634
paulabarrett@
eversheds-sutherland.com

Theo Davidson
Associate
T: +44 20 7919 4834
theodavidson@
eversheds-sutherland.com

Development	Summary	Date	Links
ICO publishes AI Toolkit	Given the prevalence of AI related developments recently, we felt it would be timely to remind readers of the ICO's AI Toolkit (first published in May 2022) which comprises a pre-recorded webinar and template risk assessment with information on the various AI lifecycle stages and links to further ICO guidance.	N/A	AI toolkit
ICO to prioritise FOI complaints which have significant public interest	The ICO has announced a new strategy for dealing with complaints made under the Freedom of Information Act ("**FOIA**") and/or Environmental Information Regulations 2004 ("**EIR**") which have significant public interest. The changes will result in these complaints being dealt with more quickly due to the implementation of a prioritisation framework. Following feedback from consultation and engagement sessions, the new criteria provides clear guidance on what constitutes a significant public interest. The ICO will aim to allocate priority cases within four weeks and fast-track up to 20% of its workload. They will also aim to close 90% of cases within six months (up from 80%). These changes are part of the ICO's wider efforts to streamline their processes for handling the large volume and complexity of FOIA / EIR complaints it receives. The changes are largely aimed at enabling the ICO to do more regulatory activity targeted at public authorities that fail to meet their transparency obligations.	28 March 2023	Statement
DPA 2018 immigration exemption still unlawful according to High Court	In R (the3million and Open Rights Group) v Secretary of State for the Home Department and others [2023] EWHC 713 (Admin) (29 March 2023), the High Court ruled that the immigration exemption in the Data Protection Act 2018, as currently drafted,	29 March 2023	Judgment ICO statement

Development	Summary	Date	Links
	is still unlawful and must be clarified. This ruling results from a case brought by the3million and the Open Rights Group. The Information Commissioner was an interested party in the claim. The Commissioner had previously raised concerns that the actions of the government did not provide enough clarity around the exemption. The ICO was an interested party in the claim having raised concerns that previous actions from the government lacked clarity, and issued a statement following the judgment.		
Guiding the use of AI in the UK	29 March 2023 saw the launch of the Government AI **white paper** to guide the use of AI in the UK. The Government hope that their approach and investment will "help create the right environment for artificial intelligence to flourish safely in the UK". Based on 5 clear principles of: – Safety security and robustness – Transparency and explainability – Fairness – Accountability and governance – Contestability and redress the government will empower existing regulators to come up with approaches to address the use of AI in their areas in the hope that this will encourage (as opposed to stifle) innovation. £2million will fund a new sandbox – a trial environment where businesses can test how regulation would be applied to AI products. Practical guidance for businesses is promised over the forthcoming months together with risk assessment templates and Government report a "warm welcome" from business for this proportionate approach following their consultation on AI conducted last year. The paper is accompanied by a further **consultation** (open until 21 June) on improving coordination between regulators and the efficacy of the approach to AI. This should help those cross-sector	29 March 2023	White paper Consultation ES briefing Report on Evidence to Support the Analysis of Impacts for AI Governance CDEI press release

Development	Summary	Date	Links

	businesses who will want a one-policy approach to complying with AI rules.
	
	Please read the **briefing from our AI colleagues Lorna Doggett and Mary Jane Wilson-Bilik**, for more commentary on the White Paper.
	
	Following on from the White Paper, the government released its final report on Evidence to Support the Analysis of Impacts for AI Governance. This report "sets out evidence to support the analysis of potential options for an AI regulatory framework in the UK". The following conclusions were reached:
	
	– a balance is required between protection of harm and the impact on industry in compliance with measures
	– increase in consumer trust could minimise the costs of regulating AI
	– further research is recommended on:
	  – the link between consumer confidence and cost savings
	  – the impact of AI regulation on research and development (R&D)
	  – the impact of AI regulation on trade
	
	A letter from the Department was also published setting out the expected role of the Digital Regulation Cooperation Forum (DRCF) which encompasses:
	
	– facilitating the cross-regulator engagement
	– horizon scanning to inform risks and opportunities
	– using their expertise from running sandbox / test environments
	
	And finally, the Centre for Data Ethics and Innovation (CDEI) confirmed their influence on the AI White Paper with a **press release** which stated that "public expectations for AI governance" were at the heart of their research report (of the same name) examining transparency, fairness and accountability.		

Development	Summary	Date	Links
Balancing privacy rights with the need to prevent crime	The ICO has investigated Facewatch, the live facial recognition technology. The technology of Facewatch allows businesses to scan people's faces in real time as they enter onto their premises, in order to protect staff, customers, and stock. If a "subject of interest" enters, the user of the system is notified. The investigation considered whether Facewatch complied with data protection legislation and raised concerns around the right of the individual to privacy versus the legitimate interests such as detection and prevention of crime. These concerns were highlighted to Facewatch who have reduced the amount of personal data they collect and the ICO is now satisfied (based on the information provided by Facewatch) that the company has a legitimate purpose for using personal data for the detection and prevention of crime. Therefore, no further regulatory action is required.	31 March 2023	Statement
Generative AI and data protection compliance	Hot on the heels of the UK White Paper on AI and the ICO's updated guidance on AI and data protection and risk toolkit, the ICO published a blog post on key questions that developers and users of Generative AI need to ask to ensure compliance with UK GDPR. The emphasis is on adopting a data protection by design and by default approach, with data protection compliance at the heart of innovation. All businesses that develop or use Generative AI should ensure that consideration of these issues is built into their strategy.	3 April 2023	Blog post
ICO responds to Government's AI white paper	The ICO published its response to the Government's AI white paper. Supportive of the Government's approach they raise the following considerations: – clarification on the role of Government and regulators in issuing guidance and advice on the law – encouraging the use of the Digital Regulation Cooperation Forum (DRCF) to promote joined-up regulatory positions	3 April 2023	Consultation response ES briefing

Development	Summary	Date	Links

	– collaboration with Government to ensure the AI principles are compatible with the data protection principles to ease compliance for businesses in the following areas:
	  – fairness – this should cover system development as well as use
	  – contestability and redress – how the ICO work with businesses on this and raises awareness of the rights people have
	  – under GDPR Art 22 – it will be a requirement for AI system operators to justify the use of AI where it has a legal or similar impact on an individual
	– joint regulatory body guidance to ensure clarity for businesses on the best practice approach to implement
	– undertaking research into the type of guidance and testing environment (sandbox) AI developers value to shape the final approach
	For more detail, please read our briefing.		

Government announces new cyber security measures	To tackle cyber threats, the government has announced new and enhanced measures to better protect their IT systems. These include: – a review of cyber security across government departments and a number of arm's length bodies – this will become an annual review – new cyber security regime known as GovAssure which encompasses a review against a good practice cyber assessment framework, third party auditing and centralised policy and guidance improving cyber resilience.	20 April 2023	Statement
National Security Cyber Centre board toolkit updated	The National Security Cyber Centre (NSCC) has launched its 'refreshed' cyber security board toolkit. Originally published in 2019, NSCC has updated its toolkit to ensure it remains relevant and framed in a language that boards are familiar with. The toolkit will help boards make informed cyber decisions that are aligned to their wider organisational risks, and ensure cyber	30 March 2023	Blog post and link to toolkit

Development	Summary	Date	Links
	security is assigned appropriate investment against other competing business demands.		
DSIT cyber security newsletter – April 2023 highlights	A new, free Check Your Cyber Security Tool has been launched by the Department for Science, Innovation and Technology to help small businesses check their cyber security as part of the Cyber Aware campaign. Cohort 7 of CyberASAP is now open for applications. Now in its seventh year, CyberASAP provides academics with the expertise, knowledge and training needed to convert their research into technologies, products and services. In March, the NHS launched its new cyber security strategy that sets out its approach to cyber resilience that will apply across both health and social care systems. This includes adult social care, primary care, secondary care and the critical supply chain. In partnership with the UK Cyber Security Council, the Department for Education is hosting three cyber security T Level workshops across England.	4 April 2023	DSIT newsletter
Parliamentary committee calls for evidence on Data Protection and Digital Information (No. 2) Bill	Experts and specialists in the field of data protection were called to submit their views on the Data Protection and Digital Information (No. 2) Bill, which is currently passing through Parliament (as reported in our previous edition of Updata), to the House of Commons Public Bill Committee. The call for evidence ran from 18 April to 13 June 2023.	18 April 2023	Press release Current version of the Bill (9 June 2023)
ICO releases an FOI self-assessment toolkit on vexatious requests	The Information Commissioner's Office ("**ICO**") has released another part of its FOI self-assessment toolkit which aims at helping public bodies with assessing and improving their compliance with their obligations under the Freedom of Information Act 2000 ("**FOIA**"). This new third topic of the toolkit covers applying the vexatious requests exemption from the obligation to release information in response to an FOIA request. Each of its five modules can be completed in stages, and generates a report providing overall ratings, suggested actions, and links to relevant ICO guidance:	**25 April 2023**	Self-assessment toolkit

Development	Summary	Date	Links
	– Module 1 – Your current position helps organisations to assess their current position in relation to applying the section 14(1) FOIA exemption – Module 2 – Identifying relevant factors covers the objective identification of serious purpose behind the request, wider public interest in the information and the impact and burden of meeting the request – Module 3 – Considering and balancing is about taking into account and weighing all relevant factors to decide whether the request imposes a disproportionate burden and is vexatious – Module 4 – Refusals and advice explains the requirements and good practice in relation to issuing refusal notices – Module 5 – Culture, learning and assurance addresses the organisation's culture of openness and transparency, training, monitoring compliance and sharing lessons learned		
CMA launches review of AI models	The Competition and Markets Authority ("**CMA**") is carrying out a review of competition and consumer protection considerations in the development and use of AI foundation models. A foundation model is a type of AI technology that is trained on a vast amount of data so that it can develop many complex capabilities, with generative AI (such as ChatGPT), writing assistants and image generation tech being examples of how AI foundation models may be deployed. This review follows on from publication of the Government's AI White Paper in March, with the CMA being tasked to focus on the areas of: – potential evolution of competitive markets for foundation models: including considering potential barriers to entry to the foundation model market itself (eg access to data and other resources) and to onward markets using foundation model capabilities – risks and benefits for both competition and consumer protection (with risks including dissemination of false and	4 May 2023	Foundation model review press release Foundation Model Taskforce press release

Development	Summary	Date	Links
	misleading information and benefits including the transformative capabilities of foundation models) – development of guiding principles to support competition and protect consumers Responses are due by 2 June 2023, with a CMA report on the findings from the review expected in September 2023. Businesses that develop and/or deploy AI foundation models should consider responding. Separately, the UK Government has announced £100 million in funding to establish a Foundation Model Taskforce. This is part of the Government's ambitions to put the UK at the forefront of global AI development and deployment, making the UK a science and tech superpower by 2030. The press release states that this kind of AI could be transformative in sectors such as healthcare and education and will boost the economy, with a prediction of it raising global GDP by 7% over a decade.		
DRCF annual report and workplan	The UK's Digital Regulation Cooperation Forum ("**DRCF**") has published its annual report for 2022/23 and its workplan for 2023/24. The DRCF is a voluntary forum comprised of the CMA, FCA, ICO and Ofcom and its purpose is to promote collaboration and coherence in digital regulation. Highlights from the last year include a joint statement from the ICO and Ofcom on data protection and online safety; a joint statement from Ofcom and the CMA on online safety and competition; a stakeholder roundtable on end-to-end encryption; fostering best practice in algorithmic processing; and joint horizon scanning for emerging tech including publication of an Insight Paper on Web 3. Work planned for the next year includes: – Online safety: codes of practice to accompany the Online Safety Bill (once this becomes law) will be prepared by Ofcom and the ICO in consultation with one another, and by Ofcom and the FCA in relation to online safety and financial promotions legislation	27 April 2023	Annual report Workplan

Development	Summary	Date	Links
	– Competition and data protection: the CMA and ICO will aim to update their joint statement on competition and data protection law, and will collaborate in this area with a focus on online advertising and online choice architecture practices that lead to competition, consumer protection and data protection harms – AI: supporting Government as it develops a framework for AI regulation, examining risks and benefits of generative AI, and further engagement with third party auditors of algorithms – Innovation: using funding from the Regulators' Pioneer Fund, design and pilot options for a multi-agency service to help digital innovators – Digital assets: joint research by the FCA and ICO to better understand consumer attitudes towards digital assets such as NFTs and crypto – Joint horizon scanning: with a focus on digital identity and business models in metaverses – Knowledge sharing: establishment of cross-regulator expert networks, with a focus on cyber security and resilience – International partnership: setting up an International Network for Digital Regulation Cooperation, initially with Australia, Ireland and the Netherlands Businesses in the fast-paced and constantly evolving tech sector will welcome a more joined-up approach by regulators to help them in navigating the often complex and overlapping regulation and guidance in this area.		
Online Safety Bill update	The Government announced a further change to the Online Safety Bill, namely the addition of an offence of encouraging or assisting a person to cause serious self-harm, whether or not they go on to do so. This reflects a Law Commission recommendation.	18 May 2023	Press release
Private Member's Bill on AI and workers' rights	The Artificial Intelligence (Regulation and Workers' Rights) Bill has been introduced to the House of Commons. This is a Private Member's Bill, which means it is highly unlikely to become law. This is recognised by Mick Whitely, the MP introducing the Bill,	17 May 2023	Hansard minutes

Development	Summary	Date	Links
	but he has introduced it in the hope of starting a conversation about how to protect workers from the threats posed by AI, both in potentially taking away jobs and in biased or discriminatory decision making.		
Cyber security playbook for smart cities	The Department for Science, Innovation and Technology has published a cyber security playbook for local authorities to help keep smart cities cyber secure. This is part of the National Cyber Strategy.	16 May 2023	Playbook
UK consumer connectable product security regime to come into force on 29 April 2024	The Government has announced that the new regime requiring manufacturers of internet or network connectable ("**smart**") products made available to consumers in the UK to ensure that these products comply with minimum cyber security standards will come into force on 29 April 2024. Details of the regime are set out in Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 (which received Royal Assent last December) and in regulations which the Government has now published in draft form: The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations. The regulations set out details of the minimum security requirements, which are based on the UK Code of Practice for Consumer IoT Security, ETSI EN 303 645 (the European Standard on Cyber Security for Consumer Internet of Things: Baseline Requirements), ISO/IEC 29147:2018 (Information technology – security techniques – vulnerability disclosure standard) and on advice from the UK's National Cyber Security Centre. When the new regime comes into force manufacturers of in-scope products will be required to: – use unique, rather than universal, default passwords for products – establish and clearly signpost a point of contact for consumers to report security issues relating to products – inform customers of the minimum period during which products will receive security updates, including as part of	29 April 2023	Press release Product Security and Telecommunications Infrastructure Act 2022 Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations

Development	Summary	Date	Links
	the information provided on websites advertising the products for sale The manufacturer, importer or distributor of a product will also have to provide a statement of compliance to confirm that the product complies with the security requirements. They will also need to take all reasonable steps to investigate and remedy any compliance failures in relation to products. Some categories of product are excluded from the regime, broadly products supplied to Northern Ireland which are subject to EU rules, charge points for electric vehicles, medical devices, smart meters and computers. Businesses that manufacture, import or distribute consumer connectable products should be reviewing and updating their current processes and procedures relating to product security now, to ensure that they are ready to comply with the new rules when they come into force in just under a year. Businesses should also be aware that the fines that may be levied for non-compliance are up to £10,000,000 or 4% of global turnover and up to £20,000 a day for ongoing non-compliance.		
Cyber security breaches survey 2023	The UK Government has published the results of its latest annual survey on the cost and impact of cyber breaches and attacks (although the report is dated April 2023, it was only released recently). The results of these surveys are used to inform Government cyber security policy. Cyber security breaches impact all organisations, so all businesses should consider the findings of this survey and the measures they could be taking to improve cyber security both in their own operations and in their supply chain. Key findings include: – smaller organisations are identifying cyber breaches and attacks less than in previous years and employing less cyber hygiene measures, with evidence suggesting that the economic climate has pushed cyber security down their agendas	19 April 2023	Survey

Development	Summary	Date	Links
	– the most common cyber threats are unsophisticated, and cyber hygiene measures to protect against them include malware protection, cloud back-ups, passwords, restricted admin rights and network firewalls – for the first time the majority of large businesses are reviewing supply chain risk, but this is still unusual across other organisations – board engagement and corporate governance is more sophisticated in larger organisations, although corporate reporting of cyber risk is uncommon across all organisations – approximately half of organisations use external information and guidance, with less than half of businesses being aware of the 10 Steps to Cyber Security guidance, 50% of medium businesses and 59% of large businesses being aware of the Cyber Essentials scheme and 27% of large businesses adhering to ISO 27001 – where external accreditation is used this is often because customers require it or because it helps organisations to produce cyber security documentation and improve their culture in this area – 21% of all business and 64% of large businesses have incident response processes in place – there tends to be a disconnect on cyber incident response between IT and other teams – cyber crime is higher among large organisations		
Department of Health and Social Care seeks public consultation on Secure Data Environments for NHS data	On 26 May 2023, the Department of Health and Social Care (DHSC) opened a public consultation regarding the use of secure data environments (SDEs) to enable secure access to NHS Health and social care data for research purposes. The consultation follows the publication of 12 policy guidelines in September 2022 which would mean that SDEs will become the 'default route for accessing NHS data.' The opportunities to access NHS data outside of these SDEs for research will be	26 May 2023	Consultation Guidelines

Development	Summary	Date	Links
	incredibly constrained and the new SDE's will need to comply with an accreditation model to ensure greater credibility and quality. It is expected that NHS organisations will maintain control over which users will have access to the datasets and for what purposes. It is permissible for NHS controlled SDEs to use commercial or academic technical solutions where it is more efficient than the NHS providing it itself. However, except in specific use cases, NHS data will no longer be hosted by commercial or academic controlled SDE's. The list of exceptions is not yet definitive but includes instances such as case by case sharing of patient-level data between NHS SDEs and SDE's in other countries and consented NHS data (such as clinical trial data) which is out of scope of for data access policy. In cases where there are existing data sharing arrangements in place, the DHSC will provide further guidance before the end of 2023. The consultation is now closed.		
High Court determines that the judicial proceedings exemption for data rights requests should be applied broadly to all judicial functions	A recent case concerns an unsuccessful subject access request ("**SAR**") by the claimant under the Data Protection Act 2018 ("**DPA**") and General Data Protection Regulation ("**GDPR**"). The claimant had been involved in litigation against a Government department and claimed against a transcription services provider and a High Court Master in respect of their refusal to provide him with his personal data, specifically for breach of the subject access provisions. The defendants had originally rejected the claimant's SAR on the basis of the exemption in paragraph 14 of Part 2 of Schedule 2 DPA, which covers "personal data processed by an individual acting in a judicial capacity, or a court or tribunal acting in its judicial capacity". The court sided with the defendants, holding that the exemption should be construed broadly to cover all manner of judicial functions, including transcription services. Its reasoning included the fact that the GDPR and DPA are not means by which to challenge judicial processes in the same way as appeals, as the claimant had attempted to do. Further, the court considered the importance of preserving the independence of the judiciary and	9 May 2023	Judgment

Development	Summary	Date	Links
	its ability to deliver judgments unfettered by the threat of litigation.		
UK-US commit to "data bridge"	Referenced as part of the Atlantic Declaration, the UK and US report they have reached an "in principle" commitment to establish the UK Extension to the EU-US Data Privacy Framework. This would mean that US companies who are approved to join the Framework would be able to receive UK personal data more easily. The Government consider that the data bridge would effectively "speed up processes, reduce costs and increase opportunity for trade". These proposals do need to be finalised and it has taken 2 years to get to this stage. Further work is required on the technical detail and the UK reviewing US data protection laws and practices. The ICO will be engaged in this process. This is not a first for the UK – we already have such data bridges with other countries such as the Republic of Korea. We will keep an eye on developments and let you know if there is final agreement on this which will mark a significant development in UK-US contracting and transfers of data.	8 June 2023	Statement
National Cyber Security Centre publishes free cyber security training packages aimed at supply chain vulnerability	Cyber-attacks resulting from weaknesses in the supply chain can have severe implications for organisations, their supply chains and ultimately their customers. Even though those implications can be costly and wide-ranging, a 2023 Department for Science, Innovation and Technology (DSIT) survey revealed that just 27% of medium and 55% of large businesses review the risks associated with their immediate suppliers. The survey also suggests that increased messaging from bodies such as the National Cyber Security Centre (NCSC) will prompt organisations to take more action in this area. Designed to aid procurement specialists, risk owners, and cyber specialists, the NCSC have released two e-learning packages. These packages are free to use and supplement the NCSC's existing guidance on mapping your supply chain and gaining confidence in your supply chain.	25 May 2023	Blog post Survey e-Learning Guidance (mapping supply chain) Guidance (confidence in supply chain) ICO report

Development	Summary	Date	Links
	The first module 'Mapping your supply chain', explores the topic of supply chain mapping and how this can be used to improve cyber security. The second module 'Gaining confidence in your supply chain' provides practical advice which can be used to assess cyber security in your supply chain by revealing how your organisation may be vulnerable to cyber-attacks.		
Portfolio of AI Assurance Techniques published by CDEI	On 7 June the Centre for Data Ethics and Innovation ("**CDEI**") announced its launch of a Portfolio of Artificial Assurance Techniques (the "**Portfolio**") The portfolio is designed for people who play a role in the design, development, deployment or procurement of AI and consists of numerous case studies which demonstrate how different AI assurance techniques are being used across a number of sectors, the case studies include examples of technical, procedural and educational approaches used to help develop reliable AI. Tools that help evaluate AI systems and whether they are aligned to current AI regulation is particularly important in improving public confidence in AI products, where there may be a lack of knowledge and trust. The techniques in the Portfolio have been mapped to the principles in the UK government's AI Regulation White Paper which outlines the current regulatory system governing AI and the outcomes driven approach to developing trustworthy AI systems (please read our briefing on this). The Portfolio provides the tools to test whether AI systems are achieving these outcomes in the real world. The Portfolio is still being developed as new case studies come to light, and the CDEI are inviting organisations to submit cases for future iterations and questions to ai.assurance@cdei.gov.uk.	7 June 2023	Press release ES AI White Paper briefing
ICO warns of "real danger" of discrimination in neurotechnology	In a blog post, the UK's Information Commissioner's Office ("**ICO**") has raised concerns that neurotechnologies could end up being inherently biased as a result of inadequate development and trialling practices. In particular, the ICO considers where devices are not trialled and assessed on a wide variety of people, inaccurate and unreliable	8 June 2023	Blog post Report

Development	Summary	Date	Links
	data may emerge. This may in turn lead to discrimination where models contain bias which lead to erroneous results and assumptions about people and communities. The ICO notes that neurodivergent people could be at particular risk of discrimination from inaccurate systems that have been trained on neuronormative patterns. The ICO is developing guidance "in the medium term" in which it will outline core legislative and technical neurotechnology definitions, highlight links to existing ICO guidance, present its views on emergent risks and provide sector-specific case studies to promote good practice by 2025. The blog also signposts to a new report *ICO tech futures: neurotechnology* which highlights future areas of potential for neurotechnologies such as the workplace and employee hiring, the sports sector, personal health and wellbeing and even marketing and video games. Organisations developing, deploying or otherwise engaging with neurotechnologies (or considering to do so) should read the ICO's report and keep an eye out for the guidance, to help understand the legal risks involved with these new technologies and what can be done to overcome them.		
Responsible access to demographic data – making AI systems fairer	The Centre for Data Ethics and Innovation (CDEI) has published a report on detecting and mitigating bias in AI systems. It brings together its research over the past 12 months looking at the challenges of accessing demographic data – an important aspect for bias detection and mitigation – and looks into two approaches for addressing these challenges: – **data intermediaries** – the potential for intermediaries to help in the collation, management and use of demographic data. However, it is early days and there is currently no service of this type being offered in the market – **data proxies** – these could help identify bias where direct collation of demographic data is not feasible. Proxies use inference to indicate bias but care is required to ensure data protection regulatory compliance	14 June 2023	Report Fairness Innovation Challenge

Development	Summary	Date	Links
	The work feeds into the AI principle of fairness and aims to support organisations as they seek to implement this principle. With a view to identifying a best practice solution the CDEI has launched a Fairness Innovation Challenge and called for use cases "to support the development of novel solutions to address bias and discrimination across the AI lifecycle".		
New ICO guidance on privacy-enhancing technologies	The ICO has issued new guidance about privacy-enhancing technologies ("**PETs**") aimed at data protection officers and others using large personal data sets in the finance, healthcare, research and central and local government sectors. The guidance is split into two parts: – the first part focuses on how PETs can be used to help achieve compliance with data protection laws, it is aimed at DPOs and those with specific data protection responsibilities at larger organisations – the second part is a more technical deep-dive and provides an introduction to the eight types of PETs that are currently available (differential privacy, synthetic data, homomorphic encryption, zero-knowledge proofs, trusted execution environments, secure multiparty computation, private set intersection and federated learning) The ICO has endorsed the use of PETs for some time now, highlighting their use for sharing personal data more safely, securely and anonymously – allowing organisations to maximise the benefits of personal data they hold and drive innovation whilst respecting people's privacy. In its accompanying blog post, the ICO also referred to its G7 counterparts and the work being done on an international scale to facilitate and drive support for responsible and innovative adoption of PETs. Organisations in the finance, healthcare, research and government sectors should be aware of this guidance as an aid for projects involving large data sets. As the ICO hopes, PETs should be considered useful tools to help organisations exploit the value of the personal data they hold, without having to sacrifice meeting their compliance obligations.	19 June 2023	Blog post Guidance

Development	Summary	Date	Links
CMA responds to Government White Paper on AI	As one of the proposed regulators for AI, the Competition and Markets Authority has now published its formal response to the Government's AI proposals. Supportive of the Government approach, the CMA emphasise: – Support for principles to be initially non statutory. By way of reminder, the principles proposed for AI cover: Safety security and robustness; Transparency and explainability; Fairness; Accountability and governance; Contestability and redress – A need to review their own remit and how this might change based on new AI policy approach (the proposed Digital Markets, Competition and Consumers Bill is welcomed and seen to benefit any future alignment) – Support for a central co-ordination function to ensure no duplication of work between regulators The successful work of the Digital Regulation Co-operation Forum (DRCF) to date and encourage Government to build on this to test how existing functions could adapt in response to the challenges posed by AI and enable further innovation and growth. They also flag how the results of a recent pilot by DCRF on multi agency advice could help inform the development of the proposed AI sandbox where AI innovators can test and understand how regulation may impact their work	1 June 2023	Statement and link to response

United States

Contributors

Michael Bahar
Co-Lead of Global Cybersecurity and Data
T: +1.202.383.0882
michaelbahar@
eversheds-sutherland.com

Sarah Paul
Partner
T: +1.212.301.6587
sarahpaul@
eversheds-sutherland.com

Alexander Sand
Counsel
T: +1.512.721.2721
alexandersand@
eversheds-sutherland.com

Rebekah Whittington
Associate
T: +1.404.853.8283
rebekahwhittington@
eversheds-sutherland.com

Mary Parks
Contract Attorney
T: +1 714 864 4236
marypark@
eversheds-sutherland.com

Mary Jane Wilson-Bilik
Partner
T: +1 202.383.0660
mjwilson-bilik@
eversheds-sutherland.com

Brandi Taylor
Partner
T: +1.858.252.6106
branditaylor@
eversheds-sutherland.com

Tanvi Shah
Associate
T: +1.858.252.4983
tanvishah@
eversheds-sutherland.com

Rachel May
Associate
T: +1.202.383.0306
rachelmay@
eversheds-sutherland.com

Development	Summary	Date	Links
Arkansas Is The Second State to Enact Social Media Restrictions for Minors	On April 4, 2023, Arkansas adopted the Social Media Safety Act. The Act bars minors from holding accounts on social media platforms without parental consent and requires social media companies to complete "reasonable age verification" via a third-	4 April 2023	SB396 as engrossed on 04-04-2023 10:19:13 (state.ar.us)

Development	Summary	Date	Links
	party vendor. Social media companies providing a "social media platform" that generates at least $100 million and more than 25% of company revenue must comply. "Social media platform" is defined as "a public or semipublic internet-based service or application that has users in Arkansas and on which a substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application." There are exemptions for email, direct messaging, licensed media streamers, B2B software, and online shopping. The Act goes into effect on September 1, 2023.		
New York City Department of Consumer and Worker Protection Adopted Final Rules for Local Law 144	Local Law 144 prohibits employers located in New York City, or employers with candidates or employees in the City from using automated employment decision tools to evaluate job candidates or employees for employee decision purposes absent bias audit and notice requirements. On April 6, 2023, the final rules promulgated pursuant to Local Law 144 were adopted. Automated employment decision tools include "any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to substantially assist or replace discretionary decision making." The employer may use the decision tool if it has been subject to a bias audit within one year prior to use, the bias audit results are on the employer or employment agency website, and the employee or candidate receives notice. Notice must inform the employee or applicant that the tool will be used, that they may request an alternative selection process, the qualifications and characteristics the tool uses to assess the employee or applicant, and the data retention policy. The final rules expand the scope of technology included under the definition of automated employment decision tools, add bias audit standards, and clarify when an employer may rely on bias audits conducted with historical data.	6 April 2023	DCWP NOA for Use of Automated Employment Decisionmaking Tools The New York City Council – File #: Int 1894-2020 (nyc.gov)

Development	Summary	Date	Links
My Health My Data Act Enacted by Washington	On April 27, 2023, Washington state enacted the My Health My Data Act (MHMDA) to expand the protections around consumer health data. The MHMDA will apply to entities not currently covered by the Health Insurance Portability and Accountability Act (HIPAA), including "any legal entity that: (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data." Consumer health data is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." Covered entities must maintain consumer health data privacy policies, obtain separate consents for collecting and sharing consumer health data, receive valid authorization prior to any sale of such data and implement data security practices to restrict access to and use of consumer health data. The MHMDA also grants consumers the rights to know whether their health data is collected, shared or sold, the right to access their health data, the right to withdraw consent for collection and sharing, and the right to deletion. The MHMDA provides for a private right of action as well as enforcement by the Washington attorney general. Plaintiffs may recover actual damages. The Act also provides for civil penalties up to $7,500. In contrast to the California Consumer Privacy Act (CCPA) and other state privacy laws, there is no revenue, data processing, or consumer threshold for an entity to fall under the MHMDA, and nonprofits appear to be in scope. It does not apply to data regulated by the federal Gramm-Leach-Bailey Act (GLBA) applicable to financial institutions (including insurance companies) or the Fair Credit Reporting Act (FCRA). Most of the MHMDA goes into effect on March 31, 2024. Small businesses have until June 2024 to comply with the MHMDA. Geofencing restrictions go into effect on July 23, 2023.	7 April 2023	MHMDA

Development	Summary	Date	Links
The National Telecommunications and Information Administration Issued a Request for Comment on AI System Accountability Measures and Policies	On April 13, 2023, the National Telecommunications and Information Administration issued a request for comment on AI system accountability measures and policies. The comments will be used for a report on AI accountability policy development. The request for comment specifically asked for comments on gaps and barriers to creating adequate accountability, the effects of accountability measures, the relationship between accountability mechanisms and compliance efforts, and how governmental and nongovernmental organizations can support AI accountability practices. Comments were due by June 12, 2023.	11 April 2023	Federal Register :: AI Accountability Policy Request for Comment
The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking to modify protections for reproductive health information under HIPAA.	On April 12, 2023, the Office for Civil Rights issued a Notice of Proposed Rule Making on proposed changes to HIPAA regulations. The proposed changes would enhance HIPAA regulations for protected health information related to reproductive health. Specifically, these proposed changes would prohibit using or disclosing protected health information either for a criminal, civil, or administrative investigation in connection with obtaining or providing reproductive health care, or to identify an individual for the purpose of initiating such an investigation.	12 April 2023	Federal Register :: HIPAA Privacy Rule To Support Reproductive Health Care Privacy
SCOTUS Holds Federal District Courts have Jurisdiction to Hear Structural Constitutional Challenges to FTC and SEC Proceedings	In *Axon Enterprise Inc. v. FTC (No. 21-86) and SEC v. Cochran (No. 21-1239)*, the Supreme Court held that federal district courts have jurisdiction to hear structural constitutional challenges to the adjudicative authority of the Federal Trade Commission (FTC) and the U.S. Securities and Exchange Commission (SEC), both of which can regulate privacy and cybersecurity. Axon Enterprise was undergoing an FTC enforcement action and Michelle Cochran was undergoing an SEC enforcement action, each before Administrative Law Judges. Both parties sued in federal district court while their respective cases were pending. In both cases, the district courts held that the agencies' enabling statutes mandated review of final agency orders by federal courts of appeals at the end of the administrative process. In other words, the district courts held that they did not have jurisdiction	14 April 2023	Axon Enterprise, Inc. v. FTC

Development	Summary	Date	Links
	to review the challenges. A circuit split resulted when, on appeal, the Ninth Circuit upheld the district court's dismissal of Axon Enterprise's appeal and the Fifth Circuit held that the SEC enabling act did not preclude jurisdiction because doing so would deny meaningful judicial review. The Supreme Court unanimously ruled that federal district courts may hear constitutional challenges to FTC and SEC authority during administrative proceedings.		
FTC, CFPD, DOJ, and EEOC Joint Statement Committing to Protect Against Bias and Unlawful Discrimination from AI	The Federal Trade Commission, Consumer Financial Protection Bureau (CFPB), Civil Rights Division of the Department of Justice (DOJ), and the Equal Employment Opportunity Commission (EEOC) issued a joint statement on April 25, 2023. The statement reiterated the agencies' commitment to preventing AI and automated decision making from perpetuating unlawful bias, unlawful discrimination, or producing other harmful outcomes. The agencies are particularly concerned about unrepresentative datasets that may correlate to protected classes, the lack of transparency around AI models, and the lack of understanding as to how AI is used.	25 April 2023	EEOC-CRT-FTC-CFPB-AI-Joint-Statement(final).pdf
Indiana Consumer Data Protection Act Signed Into Law	On May 1, 2023, the Indiana Consumer Data Protection Act (INCDPA) was signed into law. The INCDPA largely mirrors the rest of the state consumer privacy laws, especially Utah and Virginia, in terms of definitions, scope, and consumer rights provided. The Act provides for the typical consumer rights, including the right to access, the right to data portability, the right to correct, the right to delete, and the right to opt out of processing personal data. It does not apply to data regulated by the federal Gramm-Leach-Bailey Act (GLBA) applicable to financial institutions (including insurance companies) or the Fair Credit Reporting Act (FCRA). INCDPA does not provide for a private right of action and will instead be enforced by the Indiana attorney general. Civil penalties may be up to $7,500 per violation. The law goes into effect on January 1, 2026.	1 May 2023	SB0005.05.ENRH.pdf (in.gov)

Development	Summary	Date	Links
Tennessee Information Protection Act Signed Into Law	On May 11, 2023, the Tennessee Information Protection Act (TIPA) was signed into law. TIPA largely mirrors the rest of the state consumer privacy laws already enacted in terms of definitions, scope, and consumer rights provided. Unique to TIPA is the creation of an affirmative defence for controllers and processors using a written privacy policy that both provides all rights under TIPA and reasonably conforms to either the National Institution of Standards and Technology voluntary privacy framework or to another documented policy designed to safeguard consumer privacy. Additionally, TIPA includes a provision that makes certifications from both the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems legally relevant evidence of compliance. It does not apply to data regulated by the federal Gramm-Leach-Bailey Act (GLBA) applicable to financial institutions (including insurance companies) or the Fair Credit Reporting Act (FCRA). Like other consumer privacy statutes, TIPA does not include a private right of action and is instead enforced by the Tennessee attorney general. Civil penalties may be up to $7,500 per violation with treble damages for willful violations. The law goes into effect on July 1, 2024.	11 May 2023	SB0073.pdf (tn.gov)
Federal Trade Commission Panel on Cloud Computing Industry	On May 11, 2023, the Federal Trade Commission hosted a panel on cloud computing business practices to identify issues for a Request for Information related to cloud computing business practices. The panel focused in part on data security and artificial intelligence. Specifically, the panel noted that cloud computing providers are a target of bad actors, and concluded that industry and regulatory requirements, not competition among providers, will improve security practices. The panel noted that AI is the main drive shaping competition and data security in cloud computing, but that vertical integration between AI and cloud computing providers threatens innovation.	11 May 2023	

Development	Summary	Date	Links
California Privacy Protection Agency Board of Directors Met to Discuss Proposed Regulations and Priorities	At the May 15th, 2023 meeting of the board of the California Privacy Protection Agency, the board delegated authority to CPPA staff to begin developing rulemaking proposals on topics classified as "easy" and "easy to medium," as well as topics considered priorities. "Easy" and "easy to medium" topics include regulations to require businesses' consumer request denials to include information about where to submit consumer complaints, clarifying language so that consumers may request all personal information, not just 12 months of personal information, and inserting language stating that a consumer can withdraw consent at any time. The CPPA Rules Subcommittee also announced that it has begun reviewing comments provided pursuant to its request for public comments on CPRA proposed regulations for cybersecurity audits, risk assessments, and automated decision-making.	15 May 2023	Meeting Materials – California Privacy Protection Agency (CPPA) California Privacy Protection Agency Board -Potential Regulation Proposals
Equal Employment Opportunity Commission Guidance Indicates Employers are Responsible for Discrimination by AI Employment Tools	On May 18, 2023, the Equal Employment Opportunity Commission released guidance entitled "Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964." According to the EEOC, employers are generally liable for discrimination when AI tools are used to make employment decisions. Covered tools include algorithmic decision-making tools such as resume scanners, employee monitoring software, virtual chatbots, video-interviewing software that evaluates facial expressions and speech patterns, and testing software. The selection criteria used by these tools should pass muster under the disparate impact theory, meaning that the neutral criteria should not disproportionately exclude people based on a protected characteristic. The EEOC guidance encourages employers to monitor algorithmic decision-making tools for disparity and adopt alternative, less discriminatory tools when possible.	18 May 2023	Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964 | U.S. Equal Employment Opportunity Commission (eeoc.gov)
Montana Consumer Data Privacy Act Passed	On May 19, 2023, the Montana governor signed the Montana Consumer Data Privacy Act (MCDPA) into law. The MCDPA largely mirrors the rest of the state consumer privacy laws already	19 May 2023	Bill Text: MT SB384 | 2023 | Regular Session | Enrolled | LegiScan

Development	Summary	Date	Links
	enacted in terms of definitions, scope, and consumer rights provided. The Act is unique in that it applies to businesses controlling or processing the data of 50,000 Montana consumers or deriving more than 25% of gross revenue from the sale of personal data, rather than the usual requirement of 100,000 consumers or 50% of gross revenue. The MCDPA also requires teenagers between the ages of 13 and 16 to consent to sales of their personal data or use of their personal data for targeted advertising. It does not apply to data regulated by the federal Gramm-Leach-Bailey Act (GLBA) applicable to financial institutions (including insurance companies) or the Fair Credit Reporting Act (FCRA).		
Colorado Division of Insurance Proposes Significant Revisions to Its Draft Algorithm and Predictive Model Governance Regulation for Life Insurers	On May 26, 2023, the Colorado Division of Insurance (CDI) revealed, for public review and comment, a significantly revised draft of its proposed regulation (the Revised Draft Reg.) addressing the governance and risk management (GRM) framework requirements for life insurers using external consumer data and information sources (ECDIS), or algorithms and predictive models using ECDIS. The GRM framework is intended to help ensure that insurers do not unfairly discriminate against certain protected classes. Changes reflected in the Revised Draft Reg. were made in response to feedback the CDI received from stakeholders regarding the initial release of the Draft Reg. dated February 1, 2023. On June 8, 2023, CDI held another stakeholder meeting to explain the recent changes and solicit comments on the Revised Draft Reg. As requested by industry, the revised version adopts a less detailed and more principles-based framework than what was contained in the initial draft. Importantly, Section 5.A. of the Revised Draft Reg. limits the scope of the risk-based GRM framework to a determination of unfair discrimination with respect to race only, and not to the other protected classes listed in S.B. 21-169. The Revised Draft Reg. no longer contains the following: requirement that life insurers maintain comprehensive documentation regarding their use of ECDIS, or algorithms or predictive models that use ECDIS; specific information requirements for the annual report to CDI; a requirement that the insurer have clearly assigned and documented roles and	26 May 2023	DRAFT Proposed Algorithm and Predictive Model Governance Regulation

Development	Summary	Date	Links
	responsibilities for key personnel involved in the design, development, use, and oversight of ECDIS and algorithms or predictive models that use ECDIS; the Board of the life insurer is still responsible for oversight of the risk management framework, but it no longer shares responsibility with the senior executive officers of the insurer for setting and monitoring the overall AI strategy for the company; no requirement for insurers to engage outside experts where internal resources are insufficient; definitions of "Traditional Underwriting Factors" and "Disproportionately Negative Outcomes." The final regulation on the GRM framework for life insurers is expected after the June 23rd comment deadline. The draft regulation on testing for life insurers is expected in late June.		
Texas Enacts Securing Children Through Parental Empowerment Act	On June 13, 2023 Texas enacted the Securing Children Through Parental Empowerment Act (SCOPE Act). The SCOPE Act applies to digital service providers that enable users to "socially interact" with others on the service; create "public or semi-public profile[s]" on the service; and "create or post content that can be viewed by other users" and shared on message boards, chat rooms, a landing page, video channels, or a main feed. Digital service providers include websites, applications, programs, or software that collect or process personal identifying information on the internet. Providers that know minor Texas residents use their services must comply with the SCOPE Act by verifying a known minor's parent's identity and relationship to the child, develop parental tools, enable verified parents or guardians to request access to and delete a known minor's personal identifying information, limit the collection of a known minor's personal identifying information, prevent known minors from engaging in financial transactions, prohibit targeted advertising to known minors, implement content moderation, and verify age seeking to access content of adult platforms. The SCOPE Act provides for enforcement by the Texas attorney general with civil penalties of up to $10,000 per violation and actual damages. A parent or guardian of a known minor may also seek declaratory judgment or an injunction.	13 June 2023	88(R) HB 18 – Enrolled version (texas.gov)

Development	Summary	Date	Links
	The SCOPE Act will go into effect on September 1, 2024.		
The Oregon Legislature Passed the Oregon Consumer Privacy Act	On June 22, 2023, the Oregon legislature passed the Oregon Consumer Privacy Act (OCPA). If the bill is signed by the governor, it will become the country's 11th consumer privacy law. The bill is based on other consumer privacy laws already enacted, but differs in a few key areas. First, like the CCPA but unlike all other comprehensive state privacy laws, OCPA does not include an entity-level exemption for GLBA-regulated financial institutions or HIPAA-covered entities. In regards to consumer rights, OCPA includes the typical rights, as well as the right to obtain "a list of specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data." Additionally, OCPA does not exclude pseudonymous data from the data covered under the rights to access, correct, and delete. Like the other consumer privacy laws except the CCPA, the OCPA does not contain a private right of action and will instead be enforced by the attorney general with civil penalties up to $7,500 per violation (although there is a temporary 30-day cure period (expiring in January 2026) before the AG can bring enforcement action). The law goes into effect on July 1, 2024, with an exception for non-profits which will have until July 1, 2025 to comply.	22 June 2023	SB0619 (oregonlegislature.gov)

For further information, please contact:

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
T: +44 20 7919 4634
paulabarrett@eversheds-sutherland.com

Michael Bahar
Co-Lead of Global Cybersecurity and Data Privacy
T: +1 202 383 0882
michaelbahar@eversheds-sutherland.us

@ESPrivacyLaw

Editorial Team:

Theo Davidson
Associate, Editor
T: +44 20 7919 4834
theodavidson@eversheds-sutherland.com

Sophie Lewis
Trainee Solicitor
sophielewis@eversheds-sutherland.com

Finn Potter
Trainee Solicitor
finnpotter@eversheds-sutherland.com

Krishna Mistry
Trainee Solicitor
krishnamistry@eversheds-sutherland.com

Thomas Elliott
Project Co-ordinator
T: +44 1223 44 3675
thomaselliott@eversheds-sutherland.com

Joan Cuevas
Senior Legal Technologist
T: +44 20 7919 0665
joancueva@eversheds-sutherland.com

eversheds-sutherland.com

Updata Edition 20