EVERSHEDS SUTHERLAND

Updata

Your quarterly Data, Privacy and Cybersecurity update

July to September 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 July to September 2023 and is full of newsworthy items from our team members around the globe, including:

- **the launch of the EU-US Data Privacy Framework** (as well as guidance from the EDPB) and the UK Extension
- **AI and data scraping** developments, such as global data protection regulators' call to action, new rules in China on generative AI, a report from the Dutch DPA, prospective guidance in Singapore and reports in the UK from various parliamentary committees and the Competition and Markets Authority
- **information and cyber security** updates in the United States, Hong Kong and in the Chinese banking sector
- **security breach management and enforcement** updates in Ireland, Sweden, and Switzerland
- **an assortment of new laws** such as legislation implementing the EU's Whistleblowing Act in Bulgaria, Switzerland's Data Protection Act, US state laws in Colorado and Connecticut and the UK Online Safety Act
- **subject access related developments** in Austria, Germany, Ireland and Netherlands
- regulatory and legal updates regarding the **privacy and protection of children**, in France, China, Singapore and UK
- a number updates on the theme of **employee monitoring and use of company devices** such as in Germany and Italy

We hope you enjoy this edition.

Follow Eversheds Sutherland's global **Data, Privacy and Cybersecurity team** on LinkedIn.

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

General EU and International

Contributors

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

Lizzie Charlton
Data Privacy Professional Support Lawyer
T: +44 20 7919 0826
lizziecharlton@
eversheds-sutherland.com

Development	Summary	Date	Links
Data transfers update: adequacy decision opens up EU-US personal data flows once more	On 10 July 2023, the European Commission formally adopted an adequacy decision in respect of the EU-U.S. Data Privacy Framework ("**DPF**"). The decision, which took immediate effect, enables organisations to transfer personal data from the EU to US companies participating in the DPF, without, for instance, the need for SCCs or BCRs. That said, organisations should consider carefully whether they still proceed with SCCs or update any corresponding Transfer Impact Assessments ("**TIAs**"). For more information, including details of what organisations that wish to take advantage of the DPF need to do, see our Privacy team's briefing.	10 July 2023	Adequacy decision for the EU-US Data Privacy Framework Adequacy decision for safe EU-US data flows
Joint statement from international data protection regulators calls for protection of data from unlawful data scraping	A joint statement has been published by twelve national privacy / data protection authorities (Argentina, Australia, Canada, Colombia, Hong Kong, Jersey, Mexico, Morocco, New Zealand, Norway, Switzerland and the United Kingdom) calling for better protection of personal data from unlawful data scraping. Data scraping is a form of automated mass processing where (generally) publicly available information is extracted and re-used for a different purpose, most often without the data subjects' knowledge. The statement outlines global data protection principles and how to mitigate the privacy impacts and risks in relation to data scraping. The privacy risks to individuals associated with data scraping include: targeted cyberattacks; identity fraud; monitoring, profiling and surveilling individuals; unauthorised political or intelligence gathering purposes; and unwanted direct marketing.	24 August 2023	Joint statement

Development	Summary	Date	Links
	The regulators signed the statement and sent it to a number of large social media companies ("SMCs") who are invited to respond within a month to set out what measures they have in place to protect data subjects against unlawful data scraping. The statement sets out the following aims: – To outline the key privacy risks associated with data scraping – this includes targeted cyberattacks, identity fraud, monitoring, profiling and surveillance, and unwanted direct marketing or spam – To set out how SMCs and other websites should protect individuals' personal information from unlawful data scraping to meet regulatory expectations – including putting in place 'multi-layered' technical and organisational controls to mitigate any risks, such as: identifying "bot" patterns; implementing rate limiting to websites; using CAPTCHAs; taking legal action such as cease and desist letters to offenders; and notifying individuals and regulators where required – To set out steps individuals can take to minimise privacy risks – including by managing privacy settings, thinking about their online posts, and reading information, privacy notices and policies on how their data is used, shared, and disclosed Organisations operating social media platforms and other websites should take note of the recommendations in the joint statement, including those in point 2 above.		
World Ethical Data Foundation Open Suggestions Framework for building responsible AI	The World Ethical Data Foundation published an "Open Suggestions Framework" to "clarify the process of building AI by exposing the steps that go into creating it responsibly". The stated goal is "to set a healthy tone for the industry while making the process understandable by the public to illuminate how we can build more ethical AI and create a space for the public to freely ask any question they may have of the AI and data science community".	21 July 2023	Open Suggestions Framework

Development	Summary	Date	Links
	The framework consists of a series of questions that developers should ask at the stages of data selection and ingestion; creation or selection of algorithms and models; and managing test data and tagging.		
World Economic Forum releases Adopting AI Responsibly: Guidelines for Procurement of AI Solutions by the Private Sector	The World Economic Forum released *Adopting AI Responsibly: Guidelines for Procurement of AI Solutions by the Private Sector*, a guide for commercial organisations to address the ethical issues involved with the rapidly evolving adoption of AI technology with a lack of procurement tools such as benchmarks and assessment criteria. The report includes a framework for assessing and evaluating implications of acquiring AI-based solutions, guidance on the ethical issues raised by such solutions (including in relation to bias, privacy and security) and recommendations on overlay the procurement processes discussed with robust governance criteria.	20 June 2023	Adopting AI Responsibly: Guidelines for Procurement of AI Solutions by the Private Sector
EDPB adopts template complaint form and final Recommendations on application for approval and elements and principles found in Controller BCRs	The European Data Protection Board ("**EDPB**") adopted a template form for data subjects to use to lodge complaints about possible infringements in connection with the processing of their personal data in accordance with Article 77 GDPR and associated national laws. The EDPB also released a template acknowledgment of receipt of the complaint.	21 June 2023	Template complaint form Recommendations
Council of the EU and European Parliament reach provisional agreement on cybersecurity regulation for EU bodies	The Council of the EU presidency and European Parliament negotiators reached a provisional agreement on a new regulation which aims to ensure a high common level of cybersecurity across the EU institutions, bodies, offices and agencies, and to improve their resilience and incident response capacities.	26 June 2023	Press release

Development	Summary	Date	Links
	The regulation will require those within its scope to implement a cybersecurity governance, risk management and control framework. In addition, the mandate of EU's Computer Emergency Response Team will be reinforced and the team will be renamed "Cybersecurity Service for the Union institutions, bodies, offices and agencies" (albeit keeping its CERT-EU acronym). A new interinstitutional Cybersecurity Board will monitor the regulation's implementation and provide strategic direction to CERT-EU. The board will comprise representatives of all the EU institutions and advisory bodies, the European Investment Bank, the European Cybersecurity Competence Centre and the European Union Agency for Cybersecurity (ENISA), among others.		
Agreement reached on new EU Data Act	On 28 June 2023, an agreement was reached between the European Parliament and the Council of the EU on the European Data Act ("**EDA**"). The proposed law is designed to bring about a competitive data market and to make data more accessible. The EDA was proposed in February 2022 by the European Commission, arising due to various issues and confusion around, amongst other things, use and access of data generated by connected devices and a limited ability to switch between cloud service providers in the EU. The EDA seeks to boost the EU's data economy, aiming to facilitate data sharing and use, build a competitive and reliable data cloud market and giving consumers the right to switch between different cloud data service providers. The EDA will apply to manufacturers of devices, digital service providers, companies that produce connected devices and public authorities in the EU. Businesses should review their products, data processes and policies to ensure compliance. Strong security measures will need to be implemented by businesses to protect data from unauthorised access, use and disclosure. Businesses that are likely to receive data sharing requests will need to think carefully about the need to protect their trade secrets. Notably, the agreement ensures the protection of trade secrets and intellectual property rights, with safeguards in place to prevent abusive behaviours by data holders.	28 June 2023	Press release Eversheds Sutherland briefing

Development	Summary	Date	Links
	Please read our briefing for further information.		
Financial data access and payments package adopted	The European Commission adopted a package of new rules aiming to improve consumer protection and competition in the electronic payments sector. The rules will also facilitate consumers to share their data in order to access a wider range of financial products and services. You can find out more about the proposals, which include a third Payment Services Directive (PSD3), a Payment Services Regulation and a Regulation for Financial Data Access, in our July 2023 edition of Payment Matters.	28 June 2023	Press release Eversheds Sutherland Payment Matters (July 2023)
EDPB publishes new guidance for controller binding corporate rules (BCR) applications	The European Data Protection Board released its *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)*. Binding corporate rules ("**BCR**") may be used by a group of undertaking, or a group of enterprises engaged in a joint economic activity to safeguard transfers of personal data. Controller BCR are designed to cover transfers of personal data from controllers who fall within the GDPR's geographical scope (Article 3 GDPR) to other controllers or to processors within the same group established in third countries that have not been recognised as providing an adequate level of protection (Article 45 GDPR). The EDPB's recommendations aim to: provide a standard form for the application approval process for controller BCR; set out the required content for the controller BCR; set out what must be included in the controller BCR and what must be provided to the BCR lead authority in the application; and explain and discuss the requirements.	20 June 2023	Recommendations
New proposal for a Regulation on GDPR introduces changes to one-stop-shop mechanism	The European Commission proposed a new regulation to streamline co-operation between data protection authorities ("**DPAs**") in the enforcement of the GDPR in cross-border cases.	4 July 2023	Press release Proposal text

Development	Summary	Date	Links
	The proposal introduces extra steps in the process of cooperation between DPAs to help encourage agreements between the authorities and avoid the need for dispute resolution. In addition, the proposal enables complainants to express their views in relation to the relevant controller(s)/processor(s), access documents in the administrative file and challenge decisions made by the court in respect of their complaint. The proposal also contains provisions requiring the lead DPA to communicate preliminary findings to parties (including allegations and supporting evidence) as well as obligations for the EDPB to enable parties to exercise their right to be heard before a decision is taken.		
Council of Europe releases model clauses for Convention 108+ transfers of personal data	The Council of Europe released the first of three modules of model contractual clauses for the transfer of personal data. The clauses are designed to facilitate the free flow of information between parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) as amended by Protocol CETS No 223 ("**Convention 108+**") and from parties to non-parties. The clauses are for use where personal data is transferred to countries that are not signed up to Convention 108+. The clauses are recommended to be used as adopted and can be pre-approved by competent national authorities and transposed into national and regional transfer frameworks.	27 June 2023	Press release
Global Data Alliance publishes Cross-Border Data Policy Index	The Global Data Alliance published a report which evaluates the data transfer policies of nearly 100 economies to see whether they foster or constrain cross-border data flows. Using quantitative and qualitive assessment, the economies have then been ranked into four levels, creating a "cross-border data policy index." Economies ranked in Level 1 (such as the US and the UK) are those which have relatively few constraints on cross border data transfers and have been assessed to have economies which often take 'proactive steps to create a conducive environment for digital transformation.' Comparatively, Level 4 economies (China and Russia) have been assessed as having extremely restrictive	19 July 2023	Cross-Border Data Policy Index

Development	Summary	Date	Links
	cross-border data policies. The EU and its member states have been assessed as being a Level 2 economy, ie "restrictive." The report suggests that those countries ranked from Level 2-4 are less likely to benefit from the "cross-border digital transformation" and as such fail to benefit from the "educational, economic, health, safety, and security benefits of cross-border data."		
EDPB information note clarifies EU-US Data Privacy Framework transfer rules	The European Data Protection Board ("**EDPB**") published an information note to provide clarity on transfers of personal data to the US under the GDPR following the adoption of the EU-US Data Privacy Framework ("**DPF**") adequacy decision on 10 July 2023. The note is relevant for organisations transferring personal data from the EU to the US. It sets out how the DPF applies to such transfers. In addition, it explains the redress mechanism available to EU data subjects wishing to lodge a complaint under the DPF stating that individuals are encouraged to raise complaints with the US organisation in the first instance. In the area of national security (and regardless of the data transfer mechanism used), EU data subjects can make use of the new redress system where they submit a complaint to their national data protection authority who will then pass this on to the EDPB who will 'transmit the complaint' the to the US authorities.	18 July 2023	Information note
EU Cyber Resilience Act backed by MEPs	The European Parliament voted in favour of the proposed Cyber Resilience Act and negotiations with the Council will now start. The Act will set out cybersecurity requirements for products with digital components that are on the EU market. It covers similar ground to the UK's Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023. Businesses operating in both UK and EU markets will therefore need to comply with divergent regulatory regimes.	19 July 2023	Press release
Evaluation of EU Cybersecurity Regulation	The European Commission carried a call for evidence on the Cybersecurity Regulation, which set up ENISA (the European Union Agency for Cybersecurity) and the EU cybersecurity certification framework. Responses were due by 16 September.	14 July 2023	Call for evidence webpage

Development	Summary	Date	Links
EDPB statement on first review of Japan adequacy decision	The EDPB has made a *Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan* further to the European Commission's first review of the January 2019 EU-Japan adequacy decision. In the statement, the EDPB welcomes a number of developments in Japan's data protection legislation that have brought it more closely aligned to the GDPR. The statement highlights consent as a basis for transfer of personal data where there is an imabalnce of power (e.g. in an employment context), the new category of "pseudonymised personal information" and clarifying the PPC Guidelines on international transfers as issues that require further attention. It also welcomes the prospect of future cooperation between Japan and the European Commission to develop model clauses for onward transfers of EEA transferred data. EDPB agrees with the European Commission's proposal to move to an adequacy decision cycles review of four years.	18 July 2023	Statement
European Commission consults on consumer profiling techniques reporting template	The European Commission launched a consultation on the template for the description of consumer profiling techniques and audit of such descriptions required by Article 15 of the Digital Markets Act ("**DMA**"). The Commission explains the background to the consultation by emphasising how gatekeepers accumulating large volumes of data from end users can make it difficult for potential entrants and start-ups to compete with them. Further, that transparency should help avoid deep consumer profiling becoming the de facto industry standard and allow competitors to differentiate themselves through the use of superior privacy guarantees. Article 15 DMA requires gatekeepers to submit to the Commission an independently audited description of any techniques for consumer profiling applied by the gatekeeper to or across its core platform services and to make an overview of the audited description publicly available.	31 July 2023	Consultation

Development	Summary	Date	Links
	In particular, the Commission invited feedback on section 2 of the template which asks for the minimum information that gatekeepers should report to the Commission, with the aim of meeting the objectives set out in recital 72 of the DMA, including enhancing transparency and accountability regarding gatekeeper's profiling techniques, as well as facilitating fairness and contestability of their respective core platform services. This information sought by section 2 of the template is extensive, and includes details such as: – the specific purpose(s) pursued by the profiling technique(s) and for which they are used – the legal ground relied on by the gatekeeper under Article 6 GDPR and whether consent is required under points a) to d) of Article 5(2) DMA for each purpose of profiling consumers – a numbered list with a detailed description of the technical safeguards in place to avoid the presentation of advertisements on the gatekeeper's interface based on profiling of minors or children – qualitative and quantitative impact or importance of the profiling techniques in question for the business operations of the gatekeeper – actions taken to make consumers aware that they are undergoing profiling and the relevant use of such profiling The consultation was open to all, but the Commission has expressed that contributions are particularly sought from potential gatekeepers, consumer interest groups, data experts, relevant national competent authorities, platforms' business users and auditors active in relevant fields. The deadline for responses was 15 September 2023.		
EU Commission introduces common logos to be used by data intermediaries and data altruism organisations recognised under the Data Governance Act	The Data Governance Act provides a framework under which organisations can be recognised as providing data intermediation services (as provided for under the Act), and that organisations (or individuals) making data available to others can be recognised as data altruism organisations.	9 August 2023	Statement

Development	Summary	Date	Links
	Under the Act, organisations (and individuals) recognised as the above can use a logo to help people identify relevant organisations as being recognised under the Act. In August 2023 the EU Commission introduced the logos which can be used. The EU Commission also makes clear that unauthorised use of the logos is not permitted and can lead to legal consequences. For background, data intermediaries are recognised under the Act as a neutral third party providing a service enabling parties to share and receive data – without selling the data itself or using it to create or develop its own product based on the data in question. The aim is to offer a model to companies looking to share or receive data that removes concerns about a loss of commercial advantage or a risk of misuse of data by the service through which the data is shared. Organisations (or individuals) recognised under the Act as data altruists must (amongst others) be not for profit and make data available voluntarily (and without reward) in the public interest.		
European Commission Guidelines on application of NIS2 and DORA	The European Commission published guidelines on the application of the NIS2 Directive to financial entities that are also in scope of DORA (the EU Regulation on operational resilience for the financial sector).	18 September 2023	Guidelines
European Data Protection Supervisor publishes opinions on fair and proportionate use of financial and payment personal data	The European Data Protection Supervisor ("**EDPS**") published two opinions: – the proposal for a Regulation on a Financial Data Access Framework; and – the proposal for a Regulation and Directive on payment services in the EU's internal market. Both proposals aim to encourage the sharing of data to broaden financial services and products while also maintaining control by individuals or organisations over how their financial data is processed.	22 August 2023	Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market

Development	Summary	Date	Links
	The opinions call for the creation of financial data dashboards to allow users to manage their permissions, as well as monitor, restrict or grant access to their personal data/ financial data. Both proposals also clarify that granting "permission" to personal data does not mean that the user has provided their consent as per GDPR requirements. EDPS Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access aims to promote the development of 'data-driven financial services' and enabling enhanced control by consumers and firms of their financial data, empowering them to decide how their data is used. EDPS Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market aims, among other things, to enable payment service providers to process special categories of personal data given that processing such data can lead to serious breaches of rights to private life and protections to personal data. The proposal also aims to enhance fraud prevention.		
ENISA publishes report on undersea cables challenges and good practices	The European Union Agency for Cybersecurity (ENISA) published a report on undersea cables that highlights potential threats and risks to undersea cables, such as "cyber-attacks and unintentional accidents". The report also outlines steps to take to mitigate the risks of incidents. ENISA intends to follow up on the report to provide national authorities with detailed technical guidelines of the supervision of undersea cables and their associated infrastructure.	1 September 2023	Report

Development	Summary	Date	Links
	Subsea cables are vital for global internet connectivity, transmitting over 97% of internet traffic. Protecting these cables, especially in the EU, is essential due to their strategic importance. They use advanced optical fibre technology and span over 1.2 million kilometres globally. Subsea cables fall under both national and international regulations and are subject to potential threats both deliberate and, more commonly, accidental. Subsea cable landing stations, where the cables connect to land-based infrastructure, are susceptible to various attacks. Repairing these cables is complex and is reliant upon specialised ships, making a coordinated attack a significant threat to global internet connectivity. To address these challenges, countries should clarify responsibilities, enhance monitoring, detect incidents, secure landing stations, diversify cable routes, and protect cables in shallow waters. ENISA plans to provide technical guidelines to support national authorities in overseeing subsea cables and infrastructure. The report is intended for national authorities in the EU who have a responsibility to supervise public communication networks and core internet infrastructure, under the European Electronic Communications Code and the Directive on Security of Network and Information Systems (NIS2 Directive). The International Cable Protection Committee ("**ICPC**") has compiled data on 2,464 cable faults and repairs across 126 coastal jurisdictions, sourced from 12 cable maintenance agreements. These agreements include data spanning from 9 to 14 years, covering various regions such as the Atlantic, Mediterranean, North America, South East Asia, Indian Ocean, Middle East, Pacific, and more. Root causes for subsea cable incidents fall into four categories: system failures (accounting for about 4% of failures), human errors (commonly caused by marine activities like fishing and anchoring), natural phenomena (approximately 5% of incidents, including seismic activity and tsunamis), and malicious actions, which are relatively rare and not extensively documented in the ICPC data or media reports.		

Development	Summary	Date	Links
	Clarifying national authorities' roles in supervising subsea cables is essential, and exchanging protection practices with the energy sector and critical infrastructure authorities is valuable. ENISA plans to provide technical guidelines to support national authorities. Additionally, the European Commission is analysing subsea cable redundancy and resilience to identify potential high-risk points in international connectivity during major incidents.		
EU Commission designates gatekeepers under Digital Markets Act	The Digital Markets Act aims to prevent gatekeepers from imposing unfair conditions on businesses and end users, and to ensure the openness of important digital services, by setting out a list of obligations and prohibitions that firms designated as "gatekeepers" must comply with in their daily operations. On 6 September 2023, the European Commission announced that it has designated six firms as gatekeepers. These gatekeepers now have six months to prepare to comply with their obligations and the prohibitions. For more read our briefing: The European Commission designates official gatekeepers under Digital Markets Act (DMA). The EU Commission has also published a series of Q&A on the Digital Markets Act.	6 September 2023	Eversheds Sutherland briefing European Commission Q&A

Austria

Contributors

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

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

Manuel Boka
Partner
T: +43 15 16 20 160
manuel.boka@
eversheds-sutherland.at

Development	Summary	Date	Links
Austria announces major police reform to boost its ability to tackle cybercrime	The Austrian Federal Ministry of the Interior announced the "largest police reform in 20 years" with a special focus on cybercrime. This reform will establish a cybercrime competence centre with 120 employees, special cybercrime units in all regional criminal investigational offices and 38 new criminal assistance units in which IT forensic experts will support the police investigators. Further aspects of the reform involve an increased investment in equipment and infrastructure and the improvement of training through the establishment of cybercrime training centres. A further focus is centred on strengthening international cooperation and promoting prevention and awareness training in the population. The reform will be launched in early 2024 and is expected to create 700 new police jobs in the next 5 years, 300 of which will be focused on cybercrime and organized crime.	1 September 2023	Press Release (in German)
Austrian Federal Administrative Court: E-Commerce shops allowed to make marketing consent mandatory for creating user profiles	The Federal Administrative Court ruled on a complaint by a customer against an e-commerce shop operator. In the e-commerce shop, customers could either order as "guest" or create a user profile to save their data for later purchases. For	Date of Decision: 12 June 2023 Published: 20 July 2023	Decision (in German)

Development	Summary	Date	Links
	creating a user profile, the user had to consent to their data being processed for marketing purposes. A user filed a complaint at the DPA, claiming that this mandatory consent violated the GDPR requirement for consent to be freely given. The Court denied the complaint. It ruled that customers had the possibility to order as a "guest" instead, which did not require mandatory marketing consent. While ordering via a user profile can make future purchases slightly easier, ordering as a "guest" and ordering via a user profile are still to be considered essentially equivalent options. Therefore, as customers had a clear choice to order in the e-commerce shop without giving marketing consent, the complaint was denied.		
Austrian DPA rejects complaint after individual demanded payment from controllers in leiu of complaint to Autrian DPA	The complainant had submitted a subject access request to an attorney and another person (presumably their client). This case is connected to the web fonts cases that were covered in earlier Updata issues 17 and 18, but the decision does not specify the exact connection to those cases. After having been informed that the complainant's data was processed by both, the complainant informed them that their processing of the complainant's data was unlawful, and the information disclosed by them was incomplete and incorrect. The complainant demanded payment of EUR 2,900 for the annoyance and suffering felt due to this issue, otherwise a complaint would be filed with the Austrian DPA or a claim be filed at court. The Austrian DPA rejected the complaint on the basis of Article 57(4) GDPR as being manifestly unfounded, explaining that the prior demand for payment contradicted the complainant's claim of having a need for legal relief via this route. The DPA also stated that the complaint was a vexatious and disingenuous use of the Austrian DPA.	Date of Decision: 21 February 2023 Published: 1 August 2023	Decision (in German)
Austrian Federal Administrative Court rules on the extent of algorithmic transparency following GDPR access requests	The Court decided on a complaint by a data subject who had requested detailed information on the algorithm used to create their credit score. The Court confirmed that under Article 15(1)(h) GDPR, data subjects have the right to receive meaningful information about the logic involved in automated decision-making, as well as the	Date of Decision: 29 June 2023 Published: 10 August 2023	Decision (in German)

Development	Summary	Date	Links
	significance and the envisaged consequences of such processing for the data subject. However, the Court emphasized that this does not mean that the entire algorithm has to be disclosed. It is sufficient if the data subject is informed about the different variables taken into account by the algorithm and on the individual variables' influence on the calculation of the credit score (positive/negative/neutral). The exact score formulas, the computational algorithm, the statistical/computational procedure and the weighting of the data processed in the process are not covered by the right of access. The court emphasized that data subject does not have to be able to reproduce the calculation of their specific result. The data subject's complaint was therefore denied.		
Austrian Supreme Administrative Court: Right of access includes information about recipients of personal data and the specific content of the data transmitted to each recipient	A data subject filed an access request under Article 15 GDPR to a credit bureau. Amongst other information, they requested information on the specific recipients of their data and the content of the personal data transmitted to these recipients. The credit bureau agreed to provide information on the individual recipients but refused to elaborate on the content of the personal data transmitted to each individual recipient. The Supreme Administrative Court now ruled against the credit bureau. The Court stated that the right to access also includes the right to be informed about the specific content of the transmitted data to an individual recipient, insofar as it is possible to provide this information.	Date of Decision: 3 August 2023 Published: 18 September 2023	Decision (in German)
Federal Administrative Court: Handing over a business card does not constitute marketing consent	The complainant had handed over his business card to the defendant at an event. On the business card, the complainant's handwritten email address was noted. After receiving the defendant's newsletter, the complainant filed a complaint, claiming that he had never consented to receiving marketing emails. The Federal Administrative Court upheld this complaint. The Court emphasized that consent must be unambiguous to be valid. It concluded that handing over a business card is no clear consent	Date of Decision: 16 August 2023 Published: 25 September 2023	Decision (in German)

Development	Summary	Date	Links
	to receiving marketing emails. As the defendant could not prove any other consent, it was ruled that their sending of the marketing email violated the Austrian Telecommunications Act.		
Federal Administrative Court: GDPR's right of access includes information on when data was transferred to a recipient as well as contact details of the recipients	A complainant, backed by the Austrian data protection activist group NOYB, filed a complaint against a streaming provider for not providing sufficient information following a data subject access request (Article 15 GDPR). The defendant provided most of the requested information, including a list of data recipients, the complainant considered this response to be incomplete. He requested to receive contact details for each of the listed data recipients, as for many of the listed recipients this was not clear (amongst others, for several recipients the country of the recipient was listed as "Global"). Furthermore, he requested information on the timeframe when the data was transferred to these recipients, as this was required to review whether this data transfer was legal under Chapter V GDPR. The Federal Administrative Court upheld the complaint and ordered the defendant to provide the requested information. It concluded that the purpose of the right of access is to allow data subjects to to review whether their personal data has been processed in compliance with the GDPR. For this purpose, it may be required to provide information to the data subject about the timeframe of data transfers to certain recipients. The defendant was also required to provide the contact details of data recipients to enable the data subject to exercise their data subject rights to those recipients.	Date of Decision: 30 August 2023 Published: 22 September 2023	Decision (in German)

Bulgaria

Contributors

Nikolay Bebov
Partner
T: +35 9 24 39 07 07
M: + 35 989 864 1791
nikolaybebov@
eversheds-sutherland.bg

Victoria Marincheva
Senior Associate
T: + 359 2 439 07 07
M: +359 890 415 926
victoria.marincheva@
eversheds-sutherland.bg

Development	Summary	Date	Links
Commission for Personal Data Protection adopts Ordinance on the Register Keeping under the Whistleblowing Act 2023	The Bulgarian Commission for Personal Data Protection in Bulgaria adopted Ordinance No. 1 of July 27, 2023 for Keeping the Register of Reports ("**Ordinance**") under Article 18 of the Whistleblowing Act 2023. The Ordinance regulates conduct under the whistle-blowing register, which is an essential element for the accountability of the entities covered by the law (including employers from the public and private sectors), and a key aspect of the protection of whistleblowers. The adoption of the Ordinance marks the final step of the national legal framework for the protection of whistle-blowers, which commenced on 4 May 2023, entering into force.	28 July 2023	CPDP Statement

China

Contributors

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

Olivia Chen
Associate
T: +86 21 61 37 1003
oliviachen@
eversheds-sutherland.com

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

Development	Summary	Date	Links
The Provisions on the Governance of Cyberviolence Information (Draft for Comments)	The Cyberspace Administration of China introduced the Provisions on the Governance of Cyberviolence Information (Draft for Comments) ("**Provisions**") on 7 July 2023. The Provisions require the internet information service providers to: – establish management rules and platform conventions, and make them public (Section 2, Article 5) – ensure user agreements clearly define the responsibilities of users regarding the creation, reproduction, publication, and dissemination of cyberviolence information, and fulfil the corresponding management duties in accordance with the applicable laws and agreements (Section 2, Article 7) – establish and enhance their cyberviolence protection capabilities, including (among others) giving their users an option to easily disable private messages, comments, reposts and notification alerts from strangers (Section 5) The Provisions also explicitly prohibit any organisation or individual from engaging in malicious marketing practices through cyberviolence incidents, such as exploiting popularity, promoting network diversion, intentionally distorting narratives, and	23 July 2023	Draft Regulation

Development	Summary	Date	Links
	spreading and manipulating false information across multiple platforms (Section 4, Article 17). Violation of the Provisions can result in fines and/or punishment, details of which are set out in Section 6. Fines can be between 10,000-200,000 RMB depending on the nature of the breach. Internet information service providers which initiate or organize online violence, or use online violence to carry out malicious marketing and promotion, shall be severely punished in accordance with the applicable law.		
The Interim Measures for the Management of Generative Artificial Intelligence Services	The Cyberspace Administration of China and six other Chinese government authorities, have jointly released the Interim Measures for the Management of Generative Artificial Intelligence Services ("**Measures**"), which came into effect on 15 August 2023. The new regulations have been put in place in the midst of new generative AI tools being introduced by several major Chinese technology providers. **Scope** The Measures aim to regulate both service providers and users of generative AI services, where such generative AI services are provided to the public within China. "Generative AI services" means the use of generative AI technology to provide to the public in China any text, image, audio, video, or other content. "**Generative AI technology**" is broadly defined under the Measures as certain model and related technology that could generate content. Importantly, the Measures do not apply to those organisations that research, develop, and use generative AI technology but do not provide the generative AI services to the public in China. **Rules on provision and use of generative AI services** The Measures require generative AI service providers and users to, among others: – uphold the core socialist values and refrain from generating illegal content, including content that incites subversion, overturns the socialist system, endangers national security and interests, undermines the image of the country, incites separatism in the country, disrupts national unity and social	Publication Date: 10 July 2023 Effective Date: 15 August 2023	New Regulation

Development	Summary	Date	Links
	stability, promotes terrorism and extremism, ethnic hatred and discrimination, violence or obscenity, or disseminates false and harmful information; – adopt effective measures to prevent discrimination; – respect intellectual property rights and commercial ethics, and protect commercial secrets, and not exploit any advantages in algorithms, data or platforms for unfair gain; – respect the lawful rights and interests of others, and not endanger others' well-being or rights and interests in image, reputation, privacy, and personal information; and – adopt effective measures to increase transparency, accuracy and reliability in generative AI services. **Key obligations of generative AI services providers** Importantly, the Measures look at the possibility of generative AI service providers being subject to obtaining administrative permits. We anticipate that additional regulation will be introduced to provide further detail in this respect. Among the specific obligations outlined in the Measures, generative AI services providers must: – conduct pre-training and optimisation training and other data training processing activities; – establish and maintain clear, specific and operable labelling rules where data labelling is in the process of research and development of generative AI technology; – comply with their obligations as the online information content producer and personal information controller under internet content and data regulations (as applicable); – sign service agreements with their users who register for their generative AI services to clarify the rights and obligations of both parties; – clarify and disclose the user groups and use cases for their services, guide users' scientific understanding and lawful use of generative AI technology, and adopt effective measures to		

Development	Summary	Date	Links
	prevent minors from over-reliance on or addiction to generative AI services; – label generated content such as images and videos in accordance with the Provisions on the Administration of Deep Synthesis Internet Information Services; – promptly address any illegal content or illegal activities of generative AI services users and report the same to the relevant authorities; – establish mechanisms for and promptly handle complaints and reports; and – for those providing generative AI services with public opinion characteristics or the capacity for social mobilisation, carry out security assessments in accordance with relevant state provisions, and carry out filing, modification, or cancellation of filings for algorithms in accordance with the Provisions on the Management of Algorithmic Recommendations in Internet Information Services. It is worth noting that a key principle in the Measures is to regulate generative AI services in accordance with their classification and grading. It is expected that further guidelines will be issued by the relevant authorities on how to classify and grade generative AI services and regulate them accordingly. **Liability** Breach of the Measures may be penalised by the relevant authorities in accordance with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Law on the Progress of Science and Technology or other laws and regulations. Where the aforesaid laws and regulations are silent on the penalties, the relevant departments in charge may give warnings, publish criticisms, or order for corrections within a specified time limit. In serious circumstances or where requests for corrections are refused, an order may be given by the relevant authorities to suspend the provision of the related services. Where there is a violation of public security measures or where a crime is established, public security administrative sanctions or criminal liability shall be imposed in accordance with the applicable law.		

Development	Summary	Date	Links
Information Security Technology – The Technical Specification for Security Operation and Maintenance System (Draft for Comments)	The National Information Security Standardization Technical Committee released the Information Security Technology - Technical Specification for Security Operation and Maintenance System (Draft for Comments) ("**Technical Specification**") on 12 July 2023. The Technical Specification illustrates requirements on security function, internal security, security protection, and testing and assessment methods for network operation. It also provides guidelines on maintenance of access control, operation and maintenance audit, security management, and other security operation and maintenance systems. It is applicable to design, development, testing, assessment of security operation and maintenance system. According to the Technical Specification, the security function requirements require the security functions to be possessed by the security operation and maintenance system. These requirements also cover different aspects of operation and maintenance, such as user management, object management, service protocol support, access control, warning, remote access encryption, and others. Section 6 of the Technical Specification also classifies the requirements for security operation and maintenance system into basic level and enhanced level on the basis of the strength of the security functions and the level of its security, as well as the level of security protection requirements.	12 July 2023	Draft National Standard
Information Security Technology – The Framework of Network Security Product Interconnect (Draft for Comments)	The National Information Security Standardization Technical Committee released the Information Security Technology - Framework of Network Security Product Interconnect (Draft for Comment) ("**Framework**") on 19 July 2023. The Framework sets out the framework for building interconnectivity among network security products, which covers both the interconnect function and the interconnect information to guide the design, development, and application of the network security product interconnect. According to Section 4 of the Framework, the interconnect function mainly includes four categories, namely: (i) identification, (ii) protection, (iii) monitoring, and (iv) disposal. The functional interface will support the establishment of various	19 July 2023	Draft National Standard

Development	Summary	Date	Links
	functions, standardisation of the communication protocol, request the method and the required security mechanism. The interconnect information mainly includes six categories of information, namely: (i) behaviour, (ii) alarm, (iii) asset, (iv) vulnerability, (v) threat, and (vi) event. The information description needs to be provided in order to standardise the content and format of the information.		
Circular on Launching the Record-filing of Mobile Internet Applications	To combat telecom and online fraud, the Ministry of Industrial and Information Technology released the Circular on Launching the Record-filing of Mobile Internet Applications ("**Circular**") on 21 July 2023. The Circular regulates operators of mobile internet apps who engage in the provision of internet-based information services within the territory of China. It also emphasises compliance of the record-filing procedures in accordance with the Anti-Telecom and Online Fraud Law of the People's Republic of China, the Administrative Measures for Internet-based Information Services, and other provisions. Highlights of the Circular are: – Mobile app operators must accurately complete a Record-filing Form for Internet-based Information Services ("**Record-filing Form**") and the relevant letter of commitment. They must also carry out record-filing procedures with their local provincial telecommunications administrations. – Mobile app operators who intend to provide internet-based information services through their apps, such as news, publishing, education, film and television, and religion, are required to obtain prior approval from the relevant competent supervising authorities. The confirmation of approval needs to be submitted to the provincial telecommunications administrations for record-filing purposes. – Competent telecommunications authorities may adjust the content of the Record-filing Form and the relevant letter of commitment on a case-by-case basis. – The network access service providers and mobile app distribution platforms must file an application to conduct	21 July 2023	New Circular

Development	Summary	Date	Links
	verification and review through the National Internet Basic Resource Management System (ie, the ICP/IP address/domain name information record-filing management system, hereinafter referred to "**record-filing system**"). – The network access service providers and the distribution platforms must verify the user identity, the network resources, and other information of organisations or individuals who intend to engage in the provision of mobile app internet-based information services. Where the network access service providers know or should know that the provided information is inaccurate, they must not carry out record-filing procedures on behalf of those organisations or individuals. – After receiving the record-filing submission, the provincial communications administration must, within 20 working days, process the record-filing and assign the relevant filing number to the mobile app operator accordingly. They must also make the record-filing information public through the record-filing system. If the materials submitted are incomplete or inaccurate, the provincial communications administrations must not grant the record-filing and provide an explanation for their reasoning. – Mobile app operators must display their record-filing numbers in a prominent place within the mobile app and provide a link to the website of the record-filing system associated with the record-filing numbers for the public to inquire and verify the record-filing information. Distribution platforms must display the record-filing numbers and information of the mobile apps they distributed in a prominent place and submit the relevant information to the competent telecommunications authorities. – In case of any change to or deletion of the mobile app information, the mobile app operator must follow the change or deletion procedures with the original record-filing authority. Network access service providers, distribution platforms, and intelligent terminal manufacturers must not provide network access, distribution, pre-installation, and other services for the mobile app that have not carried out the record-filing procedures.		

Development	Summary	Date	Links
Measures for Data Security Management in the Business Domain (Draft for Comments)	The People's Bank of China ("**PBoC**") has introduced Measures for Data Security Management in the Business Domain (Draft for Comments) ("**Measures**") on 24 July 2023, which follows the requirements of China's key upper-level laws, including the Cybersecurity Law, Data Security Law ("**DSL**") and Personal Information Protection Law ("**PIPL**"). – **Scope of application:** the Measures apply to the data processing activities carried out by a data processor operating in the mainland Chinese banking branches under the supervision of the PBoC. – **Data classification:** Section 2 supports the in-scope organisations to determine an overall process for data security management, technical measures and data classification. Data must be classified as "general data", "important data" or "core data". Data processors must submit details of their core data (i.e. important data) to the PBoC which will create a corresponding catalogue. – **Increase of cooperation among different enforcement agencies:** Section 7 seeks to foster cooperation among different government departments by allowing the PBoC to conduct joint enforcement inspections or refer illegal activities (known or suspected) to other relevant departments. – **Export of data to overseas authorities:** Article 27 specifies that provision of data to international organizations or foreign financial authorities is subject to the approval by the PBoC, and the PBoC will process data requests from the international organisations and foreign financial authorities in compliance with applicable laws, as well as international treaties and agreements entered into or acceded to by the PRC, or on the principle of equality and reciprocity. – **Monitoring negative public opinions:** Article 41(4) and (5) require data processors to monitor public opinion on their data security practices.	24 July 2023	Draft Measures

Development	Summary	Date	Links
Guide for Developing the Minors Mode in the Mobile Internet (Draft for Comments)	The Cyberspace Administration of China published the Guide for Developing the Minors Mode in the Mobile Internet (Draft for Comments) ("**Guide**") on 2 August 2023, which upgrades the "Youth Mode" to "Minors Mode", and extends its reach from mobile apps to mobile smart terminals and app stores. – **Purpose:** The Guide aims to achieve an integration of the software and hardware, and to enable users to access the mode easily with a single click to create a secure and wholesome online environment for minors. – **Requirements:** Section 4 introduces requirements for the minors mode on mobile smart terminals, which include: (i) basic principles; (ii) usage time management; (iii) anti-bypass requirements; and (iv) supplementary requirements, while Section 5 focuses on requirements for the minors mode in mobile apps such as: (i) basic principles; (ii) content security; (iii) functions; and (iv) management of social media. – **Age-Based Restrictions:** In Article 3 of Section 3, children are categorized into 5 age groups under the Guide, namely, (i) under 3, (ii) 3-8, (iii) 8-12, (iv) 12-16, and (v) 16-18. Mobile smart terminals, applications, and application distribution platforms should provide users of different ages with information and services suitable for their physical and mental development by evaluating factors such as the product type, content, and functions based on the physical and mental development characteristics of minors at different ages. – **Parental Involvement and Responsibility:** Under Section 7 of the Guide, parents are required to sign on and sign off the Minor Modes for their children to take an active role in managing their digital experiences.	2 August 2023	Draft Regulation
The Administrative Measures for Personal Information Protection Compliance Audits (Draft for Comments)	On 3 August 2023, the Cyberspace Administration of China ("**CAC**") released the consultation draft Measures for Compliance Audit on Personal Information Protection ("**Draft Measures**") for public feedback. Under the PRC Personal Information Protection Law ("**PIPL**"), data controllers are required to conduct a compliance	3 August 2023	Draft Regulation

Development	Summary	Date	Links
	audit on their personal data processing activities in the following circumstances: – Regular compliance audits to ensure that their data processing activities are compliant with the applicable laws and administrative regulations (Regular compliance audit); and – If the regulator identifies significant risks in personal data processing activities or the personal data security incidents, the data controllers may be requested to engage professional institutions to conduct a compliance audit (Regulatory compliance audit). Prior to the release of the Draft Measures, there were no specific legal guidelines on how these compliance audits should be carried out. The Draft Measures provide guidance for the data controllers on how to implement the compliance audits. The highlights of the Draft Measures are summarised below: – **Scope:** A compliance audit under the Draft Measures is a supervisory activity that involves examining and evaluating whether the personal data processing activities of a data controller comply with the applicable laws and administrative regulations. – **Frequency:** Data controllers that process personal data of over 1 million individuals, shall conduct a compliance audit at least once a year. Data controllers that do not meet the above threshold, shall conduct a compliance audit at least once every two years. – **Form of audit:** Compliance audits initiated by a data controller itself can be conducted either (1) by the data controller internally or (2) by an appointed professional institution. – For a regulatory compliance audit requested by the regulator, the data controller must, upon receiving the regulatory request, promptly appoint a professional institution to conduct the compliance audit. – The compliance audit must be completed within 90 working days (unless the circumstances are complicated and an extension is approved by the relevant regulatory		

Development	Summary	Date	Links
	departments) and submitted to the relevant regulatory departments in a timely manner. – In addition, the data controllers must implement any rectification suggestions made by the professional institution, and report the results of rectification to the relevant regulatory departments. – **Restrictions:** In order to maintain integrity, impartiality and objectivity of the compliance audit, a professional institution may only be appointed consecutively by the same data controller no more than three times. The Draft Measures also impose restrictions on professional institutions, such as prohibition on the outsourcing of compliance audits and issuance of fraudulent reports, etc. – **Focuses of the audit:** The "Personal Information Protection Compliance Audit Focuses for Reference" annexed to the Draft Measures outlines the key areas of audit. It also imposes more specific audit requirements for compliance audits of large-scale internet platforms. – **Liability:** Penalties will be imposed on those who violate the Draft Measures (once finalised) in accordance with the PIPL and other applicable laws and regulations. Pursuant to the PIPL, those who violate the law and refuse to make corrections may be fined up to 1 million RMB. Serious non-compliance may attract a fine of up to 5% of the annual turnover of an organization or 50 million RMB, suspension or cessation of related business and revocation of relevant permits/business licence. In cases where violations constitute a crime, criminal liability may also be pursued pursuant to the applicable laws.		
Practical Guide to Cybersecurity Standards – Method for Labelling Content in Generative Artificial Intelligence Services (Draft for Comments)	The National Information Security Standardization Technical Committee released the Practical Guide to Cybersecurity Standards – Method for Labelling Content in Generative Artificial Intelligence Services (Draft for Comments) on 7 August 2023. The guide provides a method for labelling content in generative artificial intelligence services. Requirements explicit watermarks or prompt text in the display area where AI-generated content is	7 August 2023	Draft National Standard

Development	Summary	Date	Links
	presented, implicit watermarks to be detected through an interface or other tools, and metadata for AI files.		
The Provisions on Security Management of the Application of Face Recognition Technology (for Trial Implementation) (Draft for Comments)	On 8 August 2023, the Cyberspace Administration of China ("**CAC**") released the Provisions on Security Management of the Application of Face Recognition Technology (for Trial Implementation) (Draft for Comments) ("**Provisions**"). The Provisions provide that facial recognition technology can be used to process face information only when there is a specific purpose and sufficient necessity, and where strict protection measures are taken. Under Article 4, if there are other non-biometric identification technology solutions that can achieve the same purpose or meet the same business requirements, such non-biometric identification technology solutions shall be used first. Article 6 has specifies that image capture and personal identification equipment must not be installed in hotel rooms, public bathrooms, changing rooms, restrooms and other places that may infringe on the privacy of others. Article 5 of the Provisions clarifies that the use of facial recognition technology to process face information shall be subjected to the individual's separate consent or written consent in accordance with the applicable law. According to Article 15 of the Provisions, facial recognition technology users are required to conduct a personal information protection impact assessment before processing face information, and keep a record of the assessment reports for at least three years. If the purpose or method of processing facial information changes, or a major security incident occurs, users of facial recognition technology should re-assess the impact of personal information protection. The Provisions also stress in Article 16 that users who use facial recognition technology in public places, or who store face information of more than 10,000 individuals, shall complete record-filing procedures with the cyberspace authority at or above the municipal level within 30 working days. Any organisation or individual who discovers any violation of the Provisions, may file a complaint or report to the relevant authorities under Article 22.	8 August 2023	Draft Regulation

Development	Summary	Date	Links
Information Security Technology — The Security Requirements for Processing of Sensitive Personal Information (Draft for Comments)	On 9 August 2023, the National Information Security Standardization Technical Committee released the Information Security Technology — Security Requirements for Processing of Sensitive Personal Information (Draft for Comments) (the "**Security Requirements**"). The Security Requirements intend to regulate the activities of personal information processors in handling sensitive personal information. They serve as a reference for the regulatory authorities and third-party assessment organisations to supervise, manage, and assess the sensitive personal information processing activities carried out by personal information processors. Section 6 sets out the security requirements for the data processors who engaged in the activities related to the collection, storage, use, processing, transmission, provision, disclosure, and deletion of sensitive personal information. The Security Requirements outline real-life scenarios (including for example the use of biometrics) involving the processing of sensitive personal information and the applicable legal requirements. The Security Requirements also include a template for obtaining individual written consent for processing sensitive personal information.	9 August 2023	Draft National Standard
The Rules for the Acceptance and Handling of Reports on Online Infringement Information Relating to Enterprises by Website Platforms	On 10 August 2023, the Cyberspace Administration of China ("**CAC**") released the Rules for the Acceptance and Handling of Reports on Online Infringement Information Relating to Enterprises by Website Platforms (the "**Rules**"). The Rules require website platforms to promptly and accurately accept and handle reports on online infringement information relating to enterprises. Under Article 3, website platforms are required to adhere to the principles of legality, contractual obligations, classification, grading, and timely resolution. According to Article 4, website platforms should focus and give priority to accept and handle reports on the six categories of online infringement information relating to enterprises, namely: (i) counterfeit information that confuses enterprise identities; (ii) misleading information that affects the public's fair judgment, (iii) false/rumour-derived information that does not align with the	10 August 2023	New Regulation

Development	Summary	Date	Links
	enterprises' true circumstances; (iv) insulting information that defames enterprises or entrepreneurs; (v) leaked information that violates entrepreneurs' personal privacy; and (vi) other information that maliciously interferes with enterprises' normal operation and development. Website platforms are also required to promptly address misleading information, rumour-based information, insulting information, leaked information, and information that maliciously interferes with the normal operations of enterprises. Website platforms should take a graded and classified approach in handling reports of online infringement information relating to enterprises, taking into account factors such as the (i) severity of online infringement information relating to enterprises; (ii) frequency of release; (iii) impact of public opinion; and (iv) level of social harm.		
Information Security Technology — The Risk Assessment Method for Data Security (Draft for Comments)	On 21 August 2023, the National Information Security Standardization Technical Committee released the Information Security Technology — Risk Assessment Method for Data Security (Draft for Comments), which aim to support the implementation of data security risk assessment, as required in Articles 18 and 30 of the Data Security Law, and further implement the requirements of the Personal Information Protection Law.	21 August 2023	Draft National Standard
Information Security Technology – The Security Requirements for Processing of Key Data (Draft for Comments)	On 25 August 2023, the National Information Security Standardization Technical Committee released the Information Security Technology - Security Requirements for Processing of Key Data (Draft for Comment). The Security Requirements primarily specify the safety requirements of the technical aspects when key data is processed. Under Article 3.1, key data is defined as "the data in a specific field, group, or area that reaches a certain accuracy and scale that may directly endanger national security, economic operation, social stability, public health and safety, if it is leaked, tampered with, or destroyed".	25 August 2023	Draft National Standard

Czech Republic

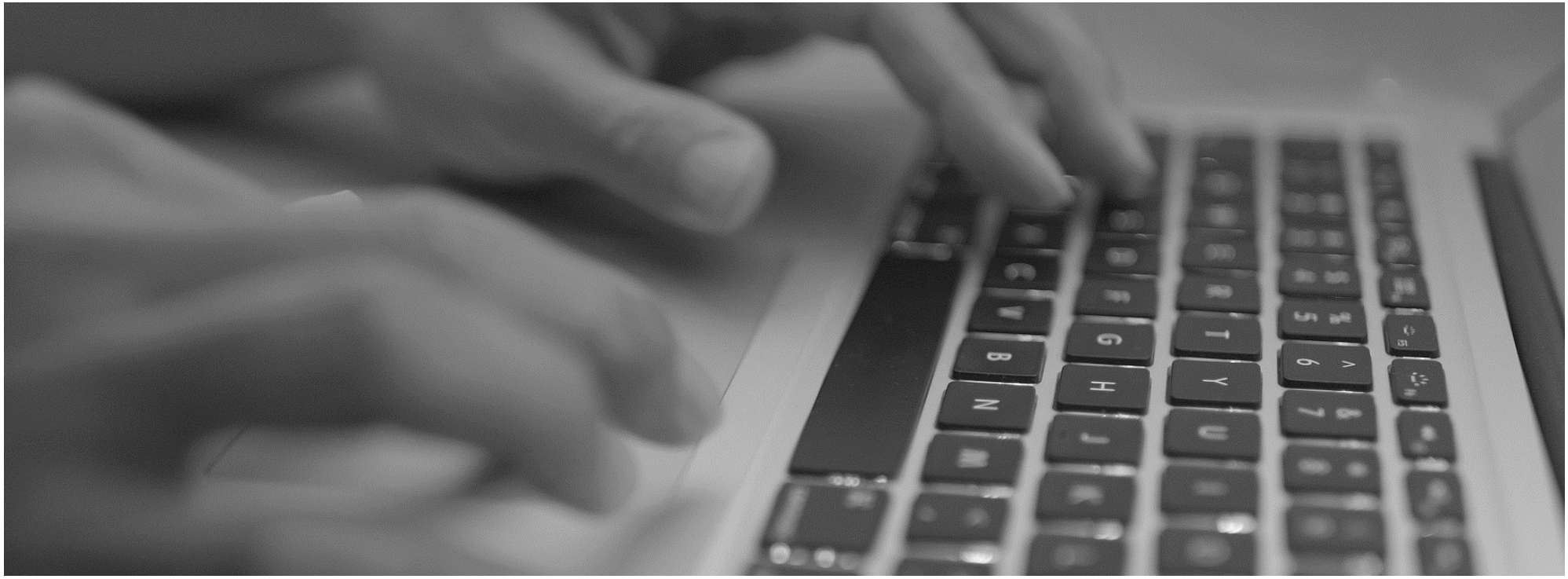
Contributors

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

Development	Summary	Date	Links
The Ministry of Justice has published the guidelines and template internal policy relating to an Internal Reporting System for the Whistleblower Protection Act	The Ministry of Justice published guidelines as well as a model internal policy for operation of the Internal Reporting System ("**IRS**") including an interpretive commentary for the Whistleblower Protection Act ("**WPA**") The WPA applies to reports containing information regarding potential illegal conduct. Reports must be made primarily through IRS or directly to the Ministry. Employers with a minimum of 50 employees are obliged to implement an IRS (either internally or through use of an external provider), whilst small and medium sized employers with up to 249 employees may choose to share an IRS or utilize an IRS operated by another company.	23 September 2023	Guidelines on Whistleblower Protection Act (in Czech) Model policy for Internal Reporting System (in Czech)
The Office for Personal Data Protection has already issued fines of nearly 4.5 million CZK this year for GDPR violations through cookies	Since the beginning of this year, the Office for Personal Data Protection ("**OPDP**") has fined various website operators a total of 4,443,000 CZK for violating the GDPR in connection with the processing of personal data through cookies. The OPDP Chairman stated that they proceeded to impose fines because operators had sufficient space and time to bring the processing of personal data through cookies into compliance with the GDPR. "We see the fines imposed primarily as a motivational and warning tool. A huge amount of personal data is processed through cookies, and this in a situation where the average visitor may not even be aware that such processing is taking place." The most frequent or most significant violations of the GDPR identified by the OPDP included:	2 August 2023	Press release (in Czech)

Development	Summary	Date	Links
	– Uploading unauthorised cookies to visitors' devices without their consent – Lack of sufficient consent to the processing of personal data – Insufficient compliance with the information obligation (insufficient classification of individual cookies or information available only in English) – Inability (or making it difficult) to withdraw consent to the processing of personal data through cookies – Placement of consent and refusal options to the processing of personal data through cookies in different layers within the cookie bar – Cookie bar not responding correctly to the individual's chosen settings of the processing of personal data via cookies.		
The Government has approved draft amendments to the Insolvency Act and the ID Cards Act reinstating use of date of birth data	On 13 September, the Government of the Czech Republic approved a draft amendment to both the Insolvency Act and the Act on ID Cards. The aim of the proposed amendment to the Act on ID Cards is to maintain the current system of entering dates of birth in ID cards, thus repealing the amendment before it had been made, which had aimed to remove this requirement. The purpose of the proposed amendments to the Insolvency Act is also to preserve the pre-existing regime of identification of debtors in insolvency proceedings by creditors based on their dates of birth and not to move to a new system of meaningless client and directional identifiers, as required by the so far ineffective earlier amendment. The Office for Personal Data Protection rejects this proposal in its entirety "as it has long held the view that the inclusion of the date of birth in ID cards leads to misuse of this data".	13 September 2023	Draft law (in Czech)
Amendment to the Czech Labour Code that has substantially facilitated the use of e-signatures and e-delivery of HR documents	The recently approved amendment to the Czech Labour Code includes substantial changes to the rules relating to the use of e-signature and the e-delivery of HR documents. It will be possible for employment and other contracts to be both delivered and completed electronically. However, these must be delivered to an electronic address of the employee which is not available to the employer (eg a private e-mail address). The	1 October 2023	Amendment to the Czech Labour Code (approved law)

Development	Summary	Date	Links
	employee will only be able to withdraw from such contract in this way within seven days of delivery if he or she has not yet started work. Stricter rules will apply to the e-signature and e-delivery of the employer's unilateral documents relating to the employment termination, including use of qualified e-signature and previous separate employee's consent with information. This amendment was effective from 1 October 2023.		



France

Contributors

Gaëtan Cordier
Partner
T: +33 1 55 73 40 73
gaetancordier@
eversheds-sutherland.com

Emmanuel Ronco
Partner
T: +33 6 15 40 00 47
emmanuelronco@
eversheds-sutherland.com

Edouard Burlet
Associate

Mélanie Dubreuil-Blanchard
Associate

Vincent Denoyelle
Partner
T: +33 1 55 73 42 12
vincentdenoyelle@
eversheds-sutherland.com

Naomi Bellaiche
Associate

Clémence Dubois Ahlqvist
Associate

Killian Lefevre
Associate

Development	Summary	Date	Links
CNIL issues technical practices guidance on data sharing via APIs	The CNIL has issued technical practices guidance relating to secure personal data sharing via application programming interfaces ("**APIs**"). Essentially, the guidance sets out the circumstances under which the use of APIs is recommended, according to a set of criteria: – the data is frequently updated; – re-users need to access it regularly; – storage of the data by the re-user is not useful (single use or continuous processing with no need for a history); – re-users do not systematically need access to all of the data, but only to a subset of the data that cannot be identified in advance; and/or – the methods used to guarantee the security of the data are likely to be updated.	7 July 2023	CNIL statement (in French) CNIL recommendation (in French) CNIL summary of the public consultation (in French)

Development	Summary	Date	Links
	Recognizing the value-added features offered by APIs in terms of security, data minimization or authorization management, the CNIL wishes to promote the use of APIs for the sharing of personal data in all the cases listed above. However, such use must be subject to taking precautions where risks are identified and the recommendations outlined by the CNIL must be followed in order to ensure compliance with data protection regulations. The guidance provides a list of risk factors allowing organisations to carry out a risk analysis and enabling them to move towards the main objectives that must be achieved in order to ensure compliance with the CNIL's recommendations. These recommendations cover all stages of the API lifecycle from design, to development to operating phases. The guidance is addressed to all types of organisations, both public and private, that are considering technical solutions to share data with another organisation. More specifically, the CNIL has distinguished three categories of actors involved in data sharing via APIs: data holders, API managers and data re-users. They are encouraged to cooperate from the outset to ensure the effective implementation of personal data protection measures and respect of data subjects' rights. The guidance provides for specific recommendations intended for each category. The CNIL's guidance was subject to a prior public consultation. The feedback collected from private entities, administrative bodies as well as research facilities was taken into account and has been summarized by the CNIL. In addition, the CNIL stated that it will publish further content aimed at specifying the use cases where its recommendations are applicable.		
Data economy: the CNIL strengthens its analysis capabilities and publishes its work program	As part of its 2022-2024 strategic plan, the CNIL has announced the creation of a new team responsible for economic analysis within its workforce. The new team is tasked with an economic analysis mission aimed at understanding the business models linked to the use of personal data and measuring the economic impact of regulatory choices. The medium-term work program of the new team will include work on: (i) dual economic and legal approach to personal data and competition; (ii) taking economic aspects into account when calculating sanctions; (iii) virtuous business models for privacy;	11 July 2023	CNIL statement (in French)

Development	Summary	Date	Links
	(iv) data brokers (so-called the secondary data market); (v) economic impact studies of the GDPR; and (vi) the economic benefits of having a data protection officer. In the opinion of the CNIL, this addition to legal, technological and ethical approaches will enrich the CNIL's perspective and expertise in protecting individuals' rights.		
The CNIL updates its whistleblowing guidelines	In 2019, the CNIL published guidelines in relation to whistleblowing procedures within organisations. Due to changes in applicable law, as a result of the implementation of the EU directive under French law regarding the protection of whistleblowers, the CNIL has updated its guidelines to account for the amended applicable regime. The updated guidelines are not binding but their implementation by organisations serves to demonstrate their compliance in terms of data processing activities in relation to whistleblowing procedures. The amended regime applicable to whistleblowing led to (i) a broader definition of reportable facts, (ii) a broader scope of individuals who may benefit from whistleblowing protection and (iii) the creation of new procedural rules. The CNIL's updated guidelines follow the same structure as the initial version and cover all reporting systems, but are limited to data protection aspects only. For example, the updated guidelines include new purposes for processing related to whistleblowing processes and recommendations on data storage.	24 July 2023	CNIL statement (in French) CNIL guidelines (in French)
Protecting minors: the CNIL issues an opinion on parental control decrees	The CNIL issued an opinion on decrees adopted within the framework of French law (no. 2022-300 of 2 March 2022) specifying the various functionalities that parental control devices will have to incorporate on connected devices (eg smartphones, computers, video game consoles, etc.). The CNIL reiterates its support for parental control systems. The introduction of such devices is an appropriate way of protecting minors from the risks to which they are exposed online, such as harassment, scams, access to unsuitable content, etc. The CNIL stresses that these tools must be developed in such a way as to ensure balance between controlling access to inappropriate content and respecting children's privacy and empowerment. They must also integrate personal data protection	31 July 2023	CNIL opinion (in French)

Development	Summary	Date	Links
	principles by both design and default. The CNIL indicates that the implementation of minimal functionalities (eg blocking the downloading of applications or content to which access is forbidden to minors) should not result in the transmission of personal data to servers.		
DPO certification: the CNIL introduces two certification frameworks	In August 2023, the CNIL introduced two certification frameworks for Data Protection Officers ("**DPOs**") to validate their skills and expertise. One of the certification scheme serves for organisations that wish to deliver certifications to individuals who want their skills recognised. The other certification scheme is designed for individuals themselves, designed to showcase their skills and knowledge in respect of data protection. This addresses the training gap for DPOs, as the GDPR lacks specific guidance on their training and qualifications. The certification frameworks outline competencies and skills required for DPOs, and the accreditation framework ensures certification bodies can assess DPOs' proficiency. Although certification is not mandatory, it empowers DPOs and strengthens organisations' commitment to data protection.	3 August 2023	CNIL statement (in French)

Germany

Contributors

Nils Müller
Partner

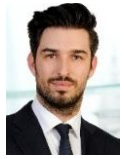
T: +49 8 95 45 65 19 4
nilsmueller@
eversheds-sutherland.com

Isabella Norbu
Associate

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

Christian Duerschmied
Associate

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



Constantin Herfurth
Senior Associate

T: +49 8 95 45 65 29 5
constantinherfurth@
eversheds-sutherland.com

Jeanette Da costa leite
Senior Associate

T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

Kevin Kurth
Associate

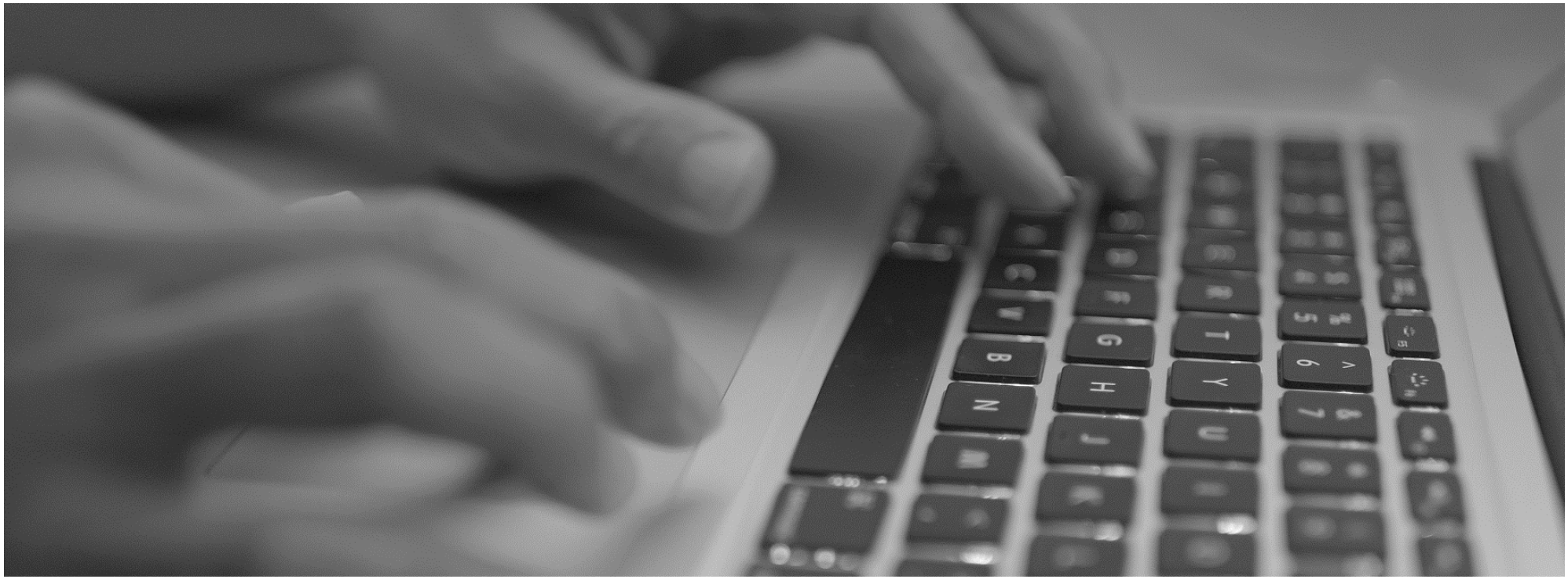
T: +49 89 54565 174
kevinkurth@
eversheds-sutherland.com

Development	Summary	Date	Links
Court rules on practice of searching work-related communication devices used by employees for private purposes	The High Labour Court of Baden-Württemberg decided that where an employer has previously allowed work-related communication devices to be used by employees for private purposes, the employer is only permitted to conduct a search of such devices in limited circumstances. Strict proportionality rules apply. Communications that have been searched on a covert basis, in the context of dismissal proceedings, may be excluded as evidence. As a rule, even a one-off search of the email account should not be carried out in an undisclosed manner. Instead, the employee must be informed about the search and the reasons and given the opportunity to store private communications in a separate folder (excluded from the search). The court also stated that in the absence of an explicitly agreed policy, employees can assume that they are allowed to use business email accounts for private purposes.	27 January 2023	Judgment (in German)

Development	Summary	Date	Links
	The key message from the case is that organisations should implement clear policies regarding the private use of company devices.		
Storage of master data of customers allowed	The Local Court Stuttgart ruled that controllers are allowed to process and, under certain circumstances, disclose personal data about an individual's address and further identity. The specific case concerned administrative offence proceedings that were opened against the cotroller – an eScooter hire company – due to a customer's violation of relevant parking regulations. The controller was unable to provide information required for the authorities to take action against the driver at fault – an address for delivery and further identification details. The controller only stored names, telephone number and e-mail address for customers. Therefore the controller, as the legal owner of the relevant eScooter, was held liable for the the parking offence. The court held that if the controller had processed the address and further identification details, then that processing would have been justified on the basis of the controller's legitimate interests and in order to fulfil its legal obligation to provide information to authorities. The court also held that this would not contravene the principle of data minimisation.	3 July 2023	Judgment (in German)
Video surveillance of employees	The Federal Court of Justice ruled that footage of an open video surveillance of employees was admissible as evidence in a dismissal case. The controller had dismissed an employee because he had finished his shift early, as evidenced by corresponding video recordings. The video surveillance was communicated to the employee by means of a corresponding pictogram and could not be contested by the employee. The use of the footage in the dismissal case was possible even if the video recording did not fully comply with the provisions of the Federal Data Protection Act or GDPR.	29 June 2023	Judgment (in German)
Misuse of rights in data subject access requests	As many other courts before it, the High Regional Court Brandenburg ruled that a data subject access request is a misuse of rights if the data subject is pursuing an alternative unjustified interest.	16 June 2023	Judgment (in German)

Development	Summary	Date	Links
	According to the court, this is the case if the data subject access request does not serve the purpose of asserting the rights of the data subject, but, for example, they want to check the legitimacy of the increase in their insurance contributions.		
Independent German Federal and State Data Protection Supervisory Authorities publishes guidance on European Commission's adequacy decision on the EU-US Data Privacy Framework	The Independent German Federal and State Data Protection Supervisory Authorities issued guidance to explain the background and content of the European Commission's adequacy decision on the EU-US Data Privacy Framework of 10 July 2023. The guidance is aimed at controllers and processors in Germany who transfer personal data to the United States, as well as at data subjects. In addition to the scope of the decision, the guidance discusses the use of alternative mechanisms for transfers to the US as well as the enforcement of rights of data subjects by the US authorities.	4 September 2023	Guidance (in German)
Saxon Commissioner for Data Protection and Transparency on the admissibility of blacklists	In her activity report for the year 2022, the Saxon Commissioner for Data Protection and Transparency commented on the admissibility of so-called blacklists under data protection law. In the case in question, the operator of an online network stored the email address of a data subject after repeated serious violations of the network's terms of use in order to be able to enforce a digital house ban. In the opinion of the authority, this is proportionate and justified on the basis of the controller's legitimate interest and takes precedence over the deletion interest of the data subject. This legal interpretation can possibly also be applied to other blacklists (e.g. in the context of email marketing), as long as there is not a large amount of data stored from the data subjects.	16 May 2023	Activity Report (in German)
Federal Ministry of the Interior publishes seeks to amend Federal Data Protection Act to restrict right of access where disclosure includes trade secrets which override data subject interest	The Federal Ministry of the Interior published a draft law amending the Federal Data Protection Act ("**BDSG**"). In addition to details on the competent supervisory authority for joint controllers, the draft contains an express restriction of the data subject's right of access if: – the information would disclose a trade or business secret of the controller or a third party; and	29 August 2023	Draft Law (in German)

Development	Summary	Date	Links
	– the interest in secrecy outweighs the interest of the data subject in receiving the information.		



Hong Kong

Contributors

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

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

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

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

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

Development	Summary	Date	Links
Privacy Commissioner's Office recommends organisations to strengthen data security measures to ensure data security	The Office of the Privacy Commissioner for Personal Data ("**PCPD**") in Hong Kong published a media statement regarding successive cyber attacks resulting in the unauthorised disclosure of personal data. The PCPD reminded all organisations, whether public/private organisations, to comply with the relevant requirements under the Personal Data (Privacy) Ordinance ("**PDPO**"), in particular, Data Protection Principle 4 of the PDPO, which requires all practicable steps be taken by data users to ensure that any personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use. The PCPD recommends that organisations holding personal data should regularly conduct data security risk assessments, put in place adequate and effective security measures to safeguard the information and communications systems and personal data in its control or possession, based on the nature, scale and complexity	22 September 2023	Media Statement

Development	Summary	Date	Links
	of the data procession activities, as well as the results of risk assessments. To strengthen data security and prevent malicious attacks on their information systems, organisations should adopt the following data security measures in a timely manner: (i) securing computer networks; (ii) regularly conducting vulnerability assessments and penetration tests; (iii) implementing patch management; (iv) encrypting data in transit and storage; (v) separating database servers from web servers by firewalls; (vi) adopting the "least privilege" principle; and (vii) timely destructing unnecessary or expired personal data.		
Privacy Commissioner's Office's response to media enquiries on data breach incident of Consumer Council	The PCPD confirmed that it had received a data breach notification from the Consumer Council and has commenced a compliance check into the incident in accordance with established procedures. The PCPD recommended organisations handling personal data should adopt the following data security measures: (i) adopting data governance and organisational measures; (ii) conducting regular risk assessments; (iii) implementing a series of technical and operational security measures; (iv) properly managing data processors; (v) taking timely remedial actions in the event of data security incidents; and (vi) regularly monitoring, evaluating and improving compliance with data security policies.	21 September 2023	Media Statement
Response of the Privacy Commissioner's Office on the Cyberport's Data Breach Incident	The PCPD received a data breach notification from Cyberport on 18 August 2023 and has commenced a compliance check into the incident in accordance with established procedures. The PCPD recommends organisations handling personal data should adopt the data security measures to safeguard data security and prevent malicious attacks on their information systems, including the measures set out in the item above in relation to PCPD's response to media enquiries on a data breach notification from the Consumer Council.	13 September 2023	Media Statement
Privacy Commissioner's Office issues 10 Tips for Users of AI Chatbots	The PCPD published a leaflet entitled "10 Tips for Users of AI Chatbots", which aims to assist users protect their personal data	13 September 2023	Media Statement Leaflet

Development	Summary	Date	Links
	privacy and provide tips on the safe use of AI chatbots. The key tips include the following: – Read the privacy policy, the terms of use and other relevant data handling policies; – Beware of fake apps and phishing websites posing as known AI chatbots; – Refrain from sharing your own personal data and others' personal data; – Guard against cybersecurity threats; – Be cautious about using the information provided by AI chatbots; and – Refrain from sharing confidential information and files.		
Privacy Commissioner's Office issues new guidance on data breach handling and data breach notifications to safeguard data security	The PCPD issued new Guidance on Data Breach Handling and Data Breach Notifications to assist organisations on how to prepare themselves in the event of a data breach. The guidance also contains practical recommendations to for handling data breaches so as to contain the damage and harm that follows from such incidents. Specifically, the guidance recommends that organisations should follow the following key steps when handling a data breach: – Step 1: immediate gathering of essential information; – Step 2: containing the data breach; – Step 3: assessing the risk of harm; – Step 4: considering whether to send data breach notifications; and – Step 5: documenting the breach. Whilst there is currently no mandatory data breach notification requirement under Hong Kong's PDPO, the guidance recommends that organisations notify the PCPD and the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects.	30 June 2023	Media Statement Guidance

Ireland

Contributors

Marie McGinley
Partner
T: +35 31 64 41 45 7
mariemcginley@
eversheds-sutherland.ie

Rosalyn English
Solicitor

Stephanie McCarthy
Trainee Solicitor

Dermot Gallagher
Trainee Solicitor

Ellie Cater
Senior Associate
T: +353 1 6644280
elliecater@
eversheds-sutherland.ie

Daniel Necz
Associate

Dhruv Khurana
Trainee Solicitor

Development	Summary	Date	Links
Eversheds Sutherland Ireland article on the Kaminski judgment and non-material damages under data protection legislation	This article provides commentary on the significance of the Kaminski v Ballymaguire Foods Limited [2023] IECC 5 decision. The judgment offers welcome guidance as to how non-material damages in data protection claims will be assessed by the Irish Courts. The level of damages payable in this case indicates that many such claims under Section 117 of the Data Protection Act 2018 will come within the jurisdiction of the District Court which, following the commencement of the Courts and Civil Law (Miscellaneous Provisions) Act 2023, will have the jurisdiction to hear these data protection claims.	25 July 2023	Eversheds Sutherland article Judgment
DPC inquiry into Galway County Council	The DPC made an inquiry examining the Galway County Council's processing operations including their use of CCTV camera in public places for the purposes of prosecuting crimes and/or other purposes. The DPC determined that the Council did not have a valid legal basis for processing personal data from CCTV cameras, Automatic Number Plate Recognition ("**ANPR**") cameras and body worn cameras. The DPC also determined that the Council did not have appropriately worded and located signage in respect of the personal data collected via CCTV cameras for purposes related to crime and law enforcement.	22 August 2023	Decision of the Data Protection Commission

Development	Summary	Date	Links
	The DPC placed a ban on the processing of personal data by the Council through body-worn, CCTV and ANPR cameras at certain locations until a valid legal basis can be identified. The DPC found that "an administrative fine would not be necessary, proportionate or dissuasive".		
DPC inquiry into online travel company's response to subject access and erasure requests	The DPC made an inquiry on foot of a complaint about a online travel company, regarding their response to a subject access request and an erasure request. On receipt of the requests, the company requested that the data subject verify their identity by providing a photocopy of their identity document, which had not previously been provided to the company. The DPC determined that the company infringed the GDPR on the following bases: – the company's request for a copy of the data subject's identity document was an infringement of the principle of data minimisation pursuant to Article 5(1)(c) of the GDPR. The DPC also found that legitimate interest was not a valid lawful basis to process personal data under Article 6(1)(f) of the GDPR, when requesting the data subject's identity document as part of their subject access request and erasure request processes. – the company did not provide the data subject with access to all of their personal data that was being processed on the date of receipt of the data subject access request, infringing Article 15(1) of the GDPR. – the company failed to provide the data subject with an access file which was concise, transparent, easily accessible and in an intelligible form, infringing Article 12(1) of the GDPR. The company failed to provide the data subject with information in relation to their actions taken on both the access and erasure requests within one month of receipt, infringing their Article 12(3) of the GDPR obligations. – The DPC ordered that the company revise their internal policies and procedures to bring their data processing into compliance.	20 July 2023	Decision of the Data Protection Commission
Data Protection Act 1988 (Section 2B) Regulations 2023	The Data Protection Act (Section 2B) Regulations 2023 (S.I no. 443 2023) commenced on the 7 September 2023 authorising the processing of sensitive personal data by the Commissioner of the	7 September 2023	Statute

Development	Summary	Date	Links
	Garda Siochana, or a member of the Garda Siochana of any rank below Commissioner acting on behalf of the Commissioner in relation to the Victim's Payments Board of Northern Ireland.		
Court and Civil Law (Miscellaneous Provisions) Act 2023	Part 12 of the Court and Civil Law (Miscellaneous Provisions) Act 2023 commenced on the 31 July 2023, amending the Data Protection Act 2018, in particular: – Enabling the DPC to prohibit the disclosure of confidential information by persons engaging with the DPC in relation to their relevant functions; – Enabling the DPC to issue reprimands to controllers and processors; and – Providing both the District Court and the Circuit Court to have jurisdiction to hear and determine actions taken by a data subject, concurrently with the High Court.	5 July 2023	Statute

Italy

Contributors

Massimo Maioletti
Partner
T: +39 06 8932 7025
massimomaioletti@
eversheds-sutherland.it

Maria Vittoria Aprigliano
Associate
T: +39 34 9972 3394
mariavittoriaaprigliano@
eversheds-sutherland.com

Edoardo Coia
Associate
T: + 39 06 8932 7034
massimomaioletti@
eversheds-sutherland.it>

Development	Summary	Date	Links
IDPA fines fashion brand EUR 240,000 for unlawful marketing activities	The Italian Data Protection Authority ("**IDPA**" or "**Authority**") fined a fashion brand for several data protection infringements in relation to its marketing activities. More specifically, the Authority found that the company had unlawfully processed a large amount of personal data, both of customers and former customers, collected through sign-ups to its e-commerce service, loyalty programme and promotional newsletter. Data collected was enriched and used for profiling activities. Also, the investigations conducted revealed that the database containing the information was accessible by any employee of the Company's shops (located in seven EU countries), from any device connected to the Internet and through a single password and a single account. Regarding the above processing activities, IDPA found: – a lack of adequate security measures; – a retention period of data collected for marketing and profiling non-compliant with the principles of storage limitation and data minimization, since it was collected for excessively long period (even more than ten years, also	5 July 2023	IDPA's measure n. 188 dated 27 April 2023 (Italian Only) IDPA's newsletter n. 508 of 28 June 2023 (Italian only)

Development	Summary	Date	Links
	considering the periods that IDPA itself recommended in its measure on loyalty cards (24 months for marketing, 12 for profiling). In light of all the above, IDPA fined the company for an amount of EUR 240.000, and made prescriptions regarding security measures, data governance, and data deletion/anonymization.		
IDPA fines company for publishing unlawfully created telephone directory on website	Following data subjects' complaints, IDPA declared a company's online collection, storage and publication of personal data via web scraping techniques to build a telephone directory to be unlawful. From the investigations conducted, IDPA found that the company relied on no appropriate legal basis for its processing activities. Moreover, the website lacked any indication of how to identify the website owner and contact the data controller. IDPA pointed out that in Italy it is prohibited to create generic telephone directories based on numbers which are not taken from the Data Base Unico, a list containing the numbers and customer data of all national fixed and mobile telephone operators. In light of the above and of the fact that the website owner had already received a sanction in 2022 for a similar infringement, IDPA imposed a fine of EUR 60,000.	17 May 2023	IDPA's measure n. 201 dated 17 May 2023 (Italian only) IDPA's newsletter n. 505 of 28 June 2023 (Italian only)
IDPA fines company for sending unlawful marketing communications	Following a complaint by a user who claimed to have received unwanted marketing e-mails, IDPA fined a company on the account of extraction of addresses from public directories, of omitted collection of data subjects' consent to send them communications. The company argued that it had processed the data based on its own legitimate interest. In its decision, the Authority reiterated that the sending of automated marketing communications is allowed only with the data subject's consent, recalling that the only exception allowed under the Italian Privacy Code concerns cases in which the data subject has provided the e-mail address in the context of a sale of similar goods or services, an exception that is not applicable to	28 June 2023	IDPA's newsletter n. 505 dated 28 June 2023 (Italian only)

Development	Summary	Date	Links
	the concerned case because there was no prior contractual relationship between the complainant and the company. IDPA also recalled that the mere inclusion of an unsubscribe link in promotional e-mails sent without consent is not sufficient to make the sending lawful. In light of the above, IDPA fined the concerned company for EUR 10,000.		
IDPA fines a company for unlawful monitoring of workers and processing of biometric data	Following a report, IDPA fined an Italian company for data protection infringements in the employment context. IDPA found that the company had installed: – a video surveillance system capable of recording live images and sound (which was accessible via the smartphone of the company's legal representative and his family) and which enabled communication with the workers via the cameras' audio playback speakers. This system was installed without compliance with Italian Workers Statute (prescribing the need for prior agreements with trade unions/authorization from the public labour authority in case of deployment of systems/devices from which employees' monitoring may derive), without providing proper privacy information notice to employees and without placing signs to indicate presence of cameras; – a geolocation application on the smartphones provided to the technical staff performing on-site interventions. IDPA found that this application continuously tracked the position of the employees via GPS, together with the date and time of the detection, thus resulting an ongoing remote control of the worker, which is forbidden under Italian employment laws. IDPA also found that the application was installed without compliance with Italian Workers Statute, and without providing proper privacy information notice to employees; – an alarm system managed through the use of biometric data, (fingerprints). IDPA noted that the processing of biometric data is only permitted if one of the conditions strictly provided for in Article 9(2) GDPR is met. In case of processing at workplace, processing biometric data is only	1 June 2023	IDPA's measure n. 231 dated 1 June 2023 (Italian only) IDPA's Newsletter n. 507 of 26 July 2023

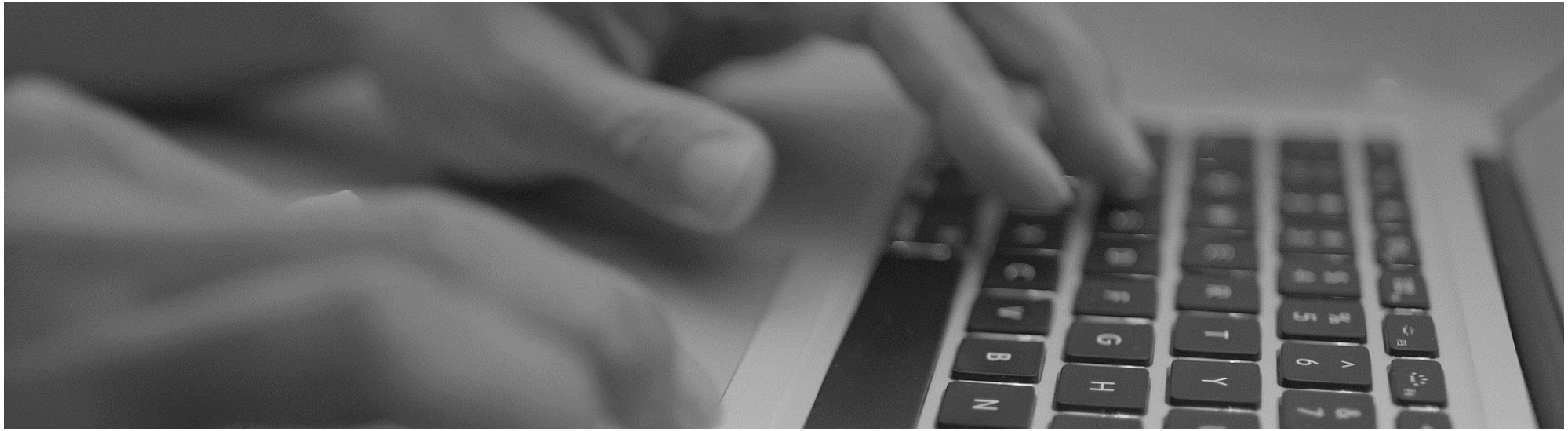
Development	Summary	Date	Links
	allowed under Article 9(2)(b) GDPR, and under specific legal provisions. These circumstances were absent in this case, making the biometric processing unlawful. Finally, the company did not provide proper privacy information notice to employees In light of the above infringements, IDPA imposed a EUR 20,000 fine on the company.		
IDPA fines company for unlawful processing of health data (providing commentary on anonymization) and incorrect classification of privacy roles	Following a report, IDPA investigated a company which was collecting health data through a project whose participants were general practitioners who had purchased a particular software application. The participating doctors, in order to join the project, were required to have a specific application add-on to the software already used and supplied by the company. Through this functionality, the data transmitted by the doctors to the company was to be automatically anonymised. In return, the doctors would receive some benefits, including financial compensation. The Authority found that the add-on functionality did not actually ensure a full anonymisation of the patients' data acquired by the doctors (IDPA cited the Article 29 Working Party guidance and provided commentary that to be truly anonymous, it must not allow single-out, likability and inference). In fact, the technique used resulted in a mere pseudonymisation, simply replacing the patients' ID with a code or encrypting them. IDPA also found inadequate identification of the legal basis of the processing pursuant to articles 6 and 9 GDPR, and that inadequate information was provided to data subjects. Therefore, the company had carried out processing in violation of the principles of lawfulness and transparency. As part of its investigations, IDPA also ascertained an incorrect identification of the privacy roles of the subjects involved in the investigated processing activties (doctors were identified as data controllers, but neither decided the means nor the purposes of the processing). On the account of the above infringements, IDPA fined the company for an amount of EUR 15,000.	1 June 2023	IDPA's measure n. 226 dated 1 June 2023 (Italian only) IDPA's Newsletter n. 507 of 26 July 2023 (Italian only)

Development	Summary	Date	Links
IDPA fines company and reiterates that despite contractual indications, privacy roles must be ascertained on a case-by-case basis	IDPA investigated a company managing motorways in Italy for unlawfully processing the data of users registered on the toll reimbursement app and found that the company had incorrectly assigned the roles of controller and processor. In fact, IDPA found that the company played the role of data controller and not of data processor, as indicated in the documentation relating to the relationship with the external provider of the app. This circumstance was reflected in the information notice provided to users, which IDPA found incorrect, as this notice was provided by a party that was not the actual data controller. Therefore, the Authority recalled that, regardless of the content of the contractual documentation, privacy roles must be identified on a case-by-case basis, taking into account the entity that determines the means and purposes of processing. In addition, IDPA found that the company was also sanctioned for not having appointed the external provider of the app as data processor. In light of the above data protection infringements, IDPA fined the company for EUR 1 million.	22 June 2023	IDPA's measure n. 264 dated 22 June 2023 (Italian only) IDPA's newsletter n. 506 of 17 July 2023 (Italian only)
IDPA fines company for failing to properly follow up on employee's access request relating to an internal investigation	Following a complaint by an employee claiming that his right of access had been infringed by the company he worked for, IDPA investigated the company on the account of failure to respond to employee's request to access personal data processed for disciplinary purposes. IDPA found that the company's failure to respond meant that the employee was unable to exercise his rights under the GDPR and was unable to fully exercise his defence rights in court proceedings to challenge his dismissal. In particular, the company denied the employee access to his company computer, lawfully requested by the latter pursuant to Article 15 GDPR, and rejected the employee's request for access to the documentation used by the employer for the dispute, because it was considered generic. The Authority held that the request for access was not generic, observing that making a response to a request for access	6 July 2023	IDPA's measure n. 290 dated 6 July 2023 (Italian only) IDPA's newsletter 509 of 11 September 2023 (Italian only)

Development	Summary	Date	Links
	conditional on the data subject's detailed indication of the documents to which access is sought does not comply with Article 15 GDPR. IDPA recalled that a request for access to data normally relates to all the data held by the data controller and that clarification should only be sought by the controller if the request is formulated in extremely general terms. The company, therefore, acknowledging the complainant's request, should have complied with the request. In addition, IDPA pointed out a violation of Article 12 of the GDPR in that the company should have acknowledged the data subject's request within one month, or informed him of any impossibility to comply with the request. The circumstance that the complainant's first request for access was sent to an address other than those indicated in the privacy notice, in fact, cannot be taken into account as a justification for a failure to reply to the data subject's requests, all the more so given that even the persons in charge of personnel management, having received the request, in any event proceeded to provide a reply without forwarding the request to the addresses indicated in the privacy notice. According to IDPA, the Company's conduct also did not appear to comply with the principle of fairness, since the data controller did not indicate the specific origin of the data used for the disciplinary complaint nor did it represent the existence of a concrete prejudice to the exercise of one of its rights. In light of the above infringements, IDPA fined the company for EUR 10,000.		
IDPA fines company for unlawful marketing communictions	IDPA made investigations, following a complaint lodged by a data subject who, despite opposing the processing by entering his data in the "**Registro Pubblico delle Opposizioni**" (Public Register of Oppositions, the Italian do-not-call list) and in the absence of prior informed consent, received undesired phone calls from the company on a daily basis. The data subject also complained that the communications had continued even after he had submitted requests to cancel the	18 July 2023	IDPA's measure n. 322 dated 18 July 2023 (Italian only) IDPA's newsletter 509 of 11 September 2023 (Italian only)

Development	Summary	Date	Links
	data and object to further processing, and that he had not received a reply to his multiple requests to exercise his rights under Articles 15, 17 and 21 of the GDPR IDPA ascertained that the company, after purchasing the data from a foreign company, contacted the data subjects to ask if they were interested in receiving commercial offers and, if so, sent them a text message with a link to a landing page where they could give their consent. This first telephone communication therefore took place without the data subjects' consent and without providing them with any information. Access to the landing pagewas conditional on the expression of interest in the company's services. In the measure, the authority clarified that the use of a mechanism that forces the user to declare an interest in a company's services in order to acquire access to the website is not lawful and that uninformed consent cannot be considered a valid premise for the marketing activity carried out by the company. In addition, IDPA rejected company's justifications that it was acting as a processor and not as a controller. In fact, the very activities carried out by the company itself, from the selection of the supplier from whom to purchase the lists to the definition of the purpose (to promote its services), up to the choice of the contact channel, make the company act as the data controller. In such respect, IDPA found the company non-compliant with its data protection obligations The Authority fined the company for an amount of EUR 40,000.		
Draft law delegating power to Italian Government to adopt implementation acts of significant EU legal acts currently under discussion before Commissions of the Italian Parliament	A draft law to delegate the Italian Government the power to adopt legislative decrees to implement several EU Directives and to amend Italian laws as needed to make them consistent with EU regulations which are becoming applicable, is currently under discussion before the Commissions of the Italian Parliament. The draft law was submitted to the Italian parliament on 27 July 2023. Parliamentary commissions exam started on 13 September 2023.	13 September 2023	Webpage of the Italian Parliament where the text draft delegation law is available (Italian only).

Development	Summary	Date	Links
	The draft delegation law includes, inter alia, delegation to implement the NIS 2 Directive, the CER Directive, and the amendments to existing laws in light of the entry into force of the DORA Regulation and Data Governance Act.		



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

Natalia Toeajeva
Junior Associate

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

Development	Summary	Date	Links
Supreme Court confirms possibility to request erasure of personal data in preliminary relief proceedings, even after expiry of 6 week time period	The Supreme Court finds that a data subject can request the erasure of personal data in preliminary relief proceedings (kort geding), even if the controller has previously rejected such request and even if the data subject did not initiate proceedings within the 6 week period provided for in Article 35 of the GDPR Implementation Act ("**UAVG**"). The appeal challenges the Lower Court's decision that the data subject had no cause of action after the 6 week period in Article 35(2) UAVG had expired. Key considerations by the Supreme Court: – Failure to initiate proceedings within the time period stated in Article 35(2) UAVG, does not automatically lead to inadmissibility in another civil action. Article 35 UAVG provides data subjects with the right to take legal action if they believe that their rights were violated under GDPR.	15 September 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	– The data subject is permitted to submit a new request to the data controller under Article 12(1) GDPR, even if no changed facts or circumstances were the basis for the repeated request. – Repeated requests from data subjects to controllers are not automatically considered unfounded or excessive, even if they have previously been rejected without changed facts or circumstances. This is in line with the GDPR's aim to provide data subjects with a high level of protection and make their rights easily accessible. – In such case, the data subject may also opt for preliminary relief proceedings – both in anticipation of a repeated request to the data controller and after such a request has been made. Consequently, no higher requirements may apply to the substantiation of the urgent interests than generally apply in preliminary relief proceedings. Nor does the data subject then have to put forward any changed facts or circumstances.		
Consultation on draft Code of Conduct for access policy to international shipping companies premises	Port Privacy B.V. focuses on privacy issues in the port of Rotterdam and has drawn up a code of conduct for the access to business premises policy of ISPS companies in the Netherlands. The Dutch Data Protection Authority ("**DDPA**") intends to approve this code of conduct. Interested parties can submit an opinion to the DDPA until 13 October 2023. ISPS companies are port companies that handle international ship traffic. For companies handling international shipping traffic, there is an obligation to certify to the International Ship and Port Facility Security Code (ISPS Code). The code of conduct relates to the access policy that applies on company premises on Dutch territory of Dutch branches of ISPS companies. The code of conduct further elaborates the GDPR obligations that ISPS companies have in this regard. ISPS companies can adopt the code of conduct. **Supervisory body** Organisations that adopt the code of conduct should also set up a supervisory body. This body monitors compliance with the code of	6 September 2023	DDPA Statement and Draft Code of Conduct (Dutch only)

Development	Summary	Date	Links
	conduct, assesses whether affiliated parties are eligible to adopt the code of conduct, and deals with complaints about breaches of the code of conduct. Port Privacy has requested the DDPA for accreditation, but the relevant supervisory body has not yet been accredited. The DDPA will approve the code of conduct on the condition that the supervisory body will be accredited.		
Consequences of invoice fraud by hacker during car purchase – no GDPR damages awarded	The case outlines the consequences of the purchase of a car, whereby the car dealership's IT environment was hacked and a fraudulent payment instruction was sent to the customer by a malicious third party, and the customer fulfilled the payment to the wrong (foreign) bank account. The customer filed two claims for damages: – Claim for pecuniary damages due to the car dealership acting in violation of the requirements of the Article 5(1)(f) and 32 GDPR, by failing to take the required security measures to ensure an adequate level of security for the processing of (sensitive) personal data of the customer. – Claim for non-pecuniary damages, arguing that the violation under GDPR by the car dealership (inadequate security measures), resulted in the malicious third party gaining access to the special category personal data of the customer, resulting in a loss of control over his personal data causing mental injury. The claim for pecuniary damages was dismissed for lack of causation and the claim for non-pecuniary damages claim was dismissed due to the lack of evidence of mental injury. Key considerations by the Court: – The car dealership had not failed to secure its IT systems from the hack. The circumstances did not justify that the car dealership was held responsible for the customer's deception. The customer should have taken reasonable precautions. – The argument that the car dealership did not do enough to secure its IT systems failed, because even with optimal security, hackers can still gain access.	22 August 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	– The customer's status as a consumer was not of any particular importance in this case, because having been a software engineer for many years, the customer should have been familiar with the risk of hacked email accounts. – The customer had not substantiated the alleged mental injury with (medical) data, on the basis of which the existence thereof can be determined according to objective standards and that he could not (further) substantiate this either.		
Dutch Court annuls fining decision of Dutch Data Protection Authority	The Court of Amsterdam annuls a fine of 525,000 EUR that was imposed by the Dutch Data Protection Authority ("**DDPA**") on a publishing company. The fine was initially imposed because the Dutch publishing company requested copies of ID documents for identification purposes when data subjects submitted their data subject requests. The publishing company successfully appealed. **GDPR violation by the publishing company** The publishing company requested a copy of data subjects' ID documentation to verify their identities as a pre-condition for (further) processing their requests for access or deletion. In case data subjects made requests outside the DPG online login environment, the ID documents were automatically requested in advance. The DDPA considered this a violation under GDPR, because it created an unnecessary barrier for data subjects involved, as the publishing company did not assess whether data subjects could be identified in a different, less intrusive ways. **Facilitating data subject rights vs. identity verification** The Court's decision took into consideration the publishing company's identification policy, which only applied when data subjects requested access to, or deletion of, personal data outside of the publishing company's digital environment. The issue was whether this policy facilitated the right to access and erasure, creating a tension between data subject rights and mandatory identity verification (Article 12(2) GDPR). The Court concluded that the DDPA applied the correct standard: *'facilitation implies the need for controllers to provide a process that allows for rights exercise without unnecessary obstacles*'. The mandatory	10 August 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	identity verification of a data subject might be an obstacle, however the obstacle should not be unnecessary. The publishing company was found to violate principles like proportionality, subsidiarity, and data minimisation by processing unnecessary data and requesting ID documentation regardless of the nature of the request. The publishing company should have considered relevant circumstances earlier in the process and the Court concluded that the publishing company's identification policy was not in line with Article 12(2) GDPR. The Court's decision aligns with previous case law and EDPB Guidelines; that requesting a copy of an ID document is acceptable, but must be necessary, proportionate and in line with national law. Key considerations by the Court: – The Court ruled that the DDPA should not have imposed the fine because it did not sufficiently consider the following circumstances: – The publishing company merely made an incorrect assessment of the required balance between data protection and facilitating other rights under the GDPR. There is no question of seriously culpable conduct. – The GDPR had only just come into effect during the period at issue and the DDPA mainly focused on providing information on the GDPR. – Based on the initial response, the DDPA failed to point out that the publishing media company's policy had to be adjusted to comply with the GDPR. – The DDPA waited months before taking any follow-up actions during the investigation. – When the initial report from the DDPA surfaced, the publishing company had already revised and amended the policy. – The violation of Article 12(2) GDPR related to a relatively limited range of requests and in the vast majority of data subject requests, there were no violations because the identity was verified in a different way.		

Development	Summary	Date	Links
Rejection of request for access on the grounds of procedural interest	The data subject exercised his right of access to find out if his personal data was shared by his employer with an external party investigating alleged inappropriate behavior by the data subject. The data subject had requested access to all personal data which (in)directly related to him as processed by the local Dutch college (employer) from the date of the investigative report up to and including, the data subject's dismissal procedure, including copies of internal notes. In response, the employer stated that they had shared name and address details with the external investigator. Any other data is not personal data and did not have to be disclosed. Further, the employer argued that it did not have to provide access to internal notes due to the ongoing dismissal procedure and its interests as an employer and protection of the alleged victim and other employees. Key considerations by the Court: – The Court found that the employer had acted in accordance with GDPR and rejected the data subject's claim for damages. – The Court acknowledged that the requested data can be regarded as personal data within the meaning of the GDPR, but that the employer may deny providing this data on the basis of the restrictions under Article 23(1)(i) and (j) GDPR. These restrictions allow the controller to balance interests and limit data subject rights, if strictly necessary and proportionate. – The legal proceedings between the employer and the data subject in an adjacent dispute and the interests of the alleged victim, outweighed the right of access. The employer sucessfully argued that it was obliged to investigate the report of inappropriate behavior in the workplace, considering the rights and interests of the person reporting the incident and other employees. – The legal obligation and guarantee for a safe and healthy working environment met the proportionality requirement. The subsidiarity requirement was also met, as the employer	3 August 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	wanted to ensure careful and objective research by engaging an external investigator.		
Company messages sent with private phones in scope of data subject access requests where no company phone	The data subject access request was aimed at gaining access to personal data processed by an organisation and included both written and electronic records, as well as communications between (former) board members, directors, (ex) employees of the organisation and other parties relating to the data subject. The defendant had only partially provided the data subject with overviews of personal data processed. The data subject argued that the defendant improperly excluded several documents from the search, including business-related SMS and WhatsApp communications which were not included. Key considerations by the Court: – During the period covered under the request, the directors did not have business phones. – The defendant enabled the possibility that business messages could be sent using private phones by not regulating the manner in which business communications may take place in that situation, eg by an internal policy. – The fact that it is customary within the organisation to communicate via business e-mail or orally does not make this any different, especially since it has been made plausible that at least the chairman had used a private telephone on several occasions for business communication. – Under these circumstances, the defendant must be considered a data controller for business messages sent by board members using private phones. Thus, the defendant should have included these messages in its search. – The Court also addressed redacting third parties' personal data from the information provided to protect their privacy, and concluded that this was justified.	17 July 2023	Court ruling (Dutch only)
Court reduces DDPA fine on Dutch Credit Registration Office	In this ruling, the Court reviewed the Dutch Credit Registration Office ("**BKR**") appeal against the administrative fine of 830,000	17 September 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	EUR imposed on it in 2019 by the DDPA for violations of Article 12(2) and (5) GDPR. According to the DDPA, the BKR wrongly charged costs for data subject requests and did not facilitate the exercise of the right of access. The Court held that the DDPA was justified in concluding that the BKR was in violation of Article 12(2) and (5) GDPR. However, considering the connection between the violations, the Court deemed the fine unreasonably high. Due to the connection of the two violations, the Court reduced the fine to 668,000 EUR. This is in fact an application of the fine policy rules as the DDPA did, but without the increase due to aggravating circumstances. Key considerations by the Court: – The Court considered Article 12 and recital 59 GDPR stating that organisations must in principle, provide means to submit access requests electronically. BKR completely excluded electronic filing, unless a paid subscription was taken, which is deemed in conflict with the right to access. The BKR should have simplified the exercise of the rights of data subjects. – The Court agreed with the DDPA that there was a serious violation given the role of the BKR and the importance of the right of access for large groups of data subjects. – It also became apparent that the Court did not agree with the BKR's definition of 'excessive request'. There is a difference between 'excessive' and above average. This will require an individual assessment of each separate request and a generic statistical average cannot suffice. – The sanction imposed must be proportionate and, according to the Court, the DDPA has extensively substantiated this and was therefore allowed to impose a fine. – Unlike the DDPA, however, the Court concluded that there were no aggravating circumstances with regards to the duration of the violation. BKR ended the violation quickly after the first report of findings was disclosed. As a result, a basic fine was sufficient.		

Development	Summary	Date	Links
DDPA publishes first report on algorithm risks	The new Algorithm Coordination Department of the DDPA published their first report on Algorithm Risks in the Netherlands. The Dutch Algorithm Risks report is a first total overview of developments, risks and challenges, brought together from an overarching risk perspective. In terms of exercising control over algorithms and artificial intelligence ("**AI**"), two challenges arise: – the speed at which AI innovations are implemented in society, such as smart chatbots; and – high risk algorithms that have a major impact on people's lives such as when applied to assessing applicants, detecting fraud, assessing customers for purchases or loans. Risks include for example, the risk of discrimination, unfair outcomes, deception and lack of transparency and how to interpret outcomes. In order to fully take advantage of the opportunities, the risks must be well managed. As long as risks cannot be managed, organisations, would be wise to exercise with caution. Awareness on this topic is increasing, but many governments and companies are still looking for the right way to utilise AI and algorithm driven technologies. Other than awaiting regulation, the report states that companies can already take steps by deploying more staff and training in the monitoring of algorithms. **Focus on high-risk systems** The DDPA further calls upon the government to give government organisations one year to complete the algorithm register disclosing all high-risk algorithms. Going forward, the DDPA will publish a Dutch Algorithm Risk Report every six months, in order to provide a picture of recent developments, current risks and associated challenges.	17 July 2023	DDPA Statement and Report (Dutch only)
Court rules Dutch bank has legitimate interest in processing customer data for incident registers	The central question was whether the entry of the customer's personal data in incident registers of a Dutch bank was necessary for the bank's legitimate interests. More specifically, whether the customer was involved in a fraud case in 2019 - defrauding	11 September 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	another customer of the bank - and whether his personal data could be registered in relation thereto. Key considerations by the Court: – The Court found that the bank had sufficiently substantiated that the customer was involved as a "money mule" in a fraud case, also considering that the customer offered insufficient evidence to oppose the bank's claim, because there was no clear explanation for the suspicious actions performed with his debit card. The bank thus had a legitimate interest in processing the customer's personal data in the incident registers. – However, the Court considered registration in both registers for the maximum period of eight years to be disproportionate, given the serious consequences for the customer in the long term. – Taking everything into account, the Court considered a retention period for the entries until December 31 2023 to be proportionate, after which the bank was ordered to delete the customer's personal data from the registers.		
Unlawful processing justifies erasure of personal data from the Fraud Alert Register of the Dutch Tax Authority	An individual was wrongly included in the Dutch Tax Authority's Fraud Alert Register ("**FSV**"), after which the data subject submitted several data subject requests: access, rectification, deletion and objection. The Dutch Tax Authority partly granted the request for access, which revealed that the data subject was listed in the FSV and rejected the requests for rectification, erasure and objection. The data subject appealed these decisions. This ruling confirms previous Dutch case law on the nature and scope of the right of access, clarified that the right of access applies in principle only to personal data of the data subject himself and not to personal data of third parties and clarified the right to erasure. **Request for access** The data subject had received a copy of the FSV registration with redacted data. It follows from the copy that the information entered under the "source" heading, namely the word "query", was mistakenly not provided. Query refers to the searches that	6 July 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	the Tax Authority performs to analyse large quantities of tax returns for possible inaccuracies. Therefore, the Tax Authority acted in violation of Article 15 GDPR by not providing access to all of the data subject's personal data in the first place. The Court found that the Tax Authority was right to redact the data from the copy as this included personal data of third parties that could not (further) identify the data subject. As it did not concern personal data of the data subject, the redacted data did not fall within the scope of the right of access of Article 15 GDPR. **Request for erasure** The Court found that the data subject's personal data had been unlawfully processed in the register, giving the data subject, in principle, the right to erasure of his personal data in line with Article 17(1)(d) GDPR. In this case, it was not necessary to: – retain the data subject's personal data for handling the data subject requests; – retention was not necessary for ongoing legal proceedings; and – the Court did not consider the retention of personal data necessary for archiving and investigation purposes. The Tax Authority was ordered to delete the personal data within one month in line with Article 12(3) GDPR.		

Poland

Contributors

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

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

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

Development	Summary	Date	Links
Supreme Administrative Court upholds Poland's first Data Protection Authority decision imposing a fine under GDPR	In a case that had started in March 2019 and had resulted in the first fine imposed in Poland under GDPR, the Supreme Administrative Court ("**SAC**") dismissed the controller's cassation appeal. Consequently, SAC shared the opinion of the Polish DPA, that processing of personal data collected from the publicly available registers require providing data subjects with the relevant privacy notice. The DPA's decision back in 2019 imposed a fine of 220,000 EUR on the private sector company for processing personal data obtained from publicly available public registries, without complying with the information obligation pursuant to Article 14 GDPR. The company appealed to the Voivodship Administrative Court ("**VAC**"), which partially agreed with the DPA in its ruling of 11 December 2019 (cf. II SA/Wa 1030/19). The court ruled that the company was should have provide with relevant privacy notice those data subject who remained active in the registries but overturned the decision as to the records no longer in force. Consequently the number of data subject affected by the company's processing diminished which in turn impacted the fine.	19 September 2023	DPA announcement (in Polish only)

Development	Summary	Date	Links
	In its cassation appeal the company invoked Article 14(5)(b) GDPR ie exemption from fulfilling the information obligation when it proves impossible or would involve a disproportionate effort. SAC (cf. III OSK 2538/21) disagreed with this line of argument and stressed that transparency of processing is a principle under GDPR, and any exceptions to this principle, should be interpreted narrowly and, as a rule, should be applied when processing data for public purposes, particularly statistical, research, archival or historical purposes. In the result the prior VAC ruling has been upheld, leaving the DPA to reconsider its decision with regard to the processing of data of data subjects that are no longer active in public registries, and with regard to the amount of the administrative penalty imposed.		
DPA investigating use of ChatGPT	The DPA is investigating a complaint against a company that owns and operates a generative AI product. The list of the complainant's allegations is long: from non-complying with the information obligation, not satisfying their request to rectify personal data after the AI product generated false information on the complainant, to infringing the purpose limitation rule (Article 5(1)(b) GDPR) and transparency obligation (Article 12 GDPR), by responding to the data subject's request in evasive and misleading manner. The complainant states that the company obtained their data in 2021 and has not provided them with information regarding the sources they collected their data from, nor of the recipients of the data. So far, the DPA announced they will provide the company with a set of questions to answer, to investigate the numerous issues raised by the complainant.	20 September 2023	DPA announcement (in English)
Polish Data Protection Authority's annual report for 2022	Polish DPA published its annual report for 2022 summarizing its activities over the past year. The report shows that the DPA imposed 20 administrative fines, 2 more than in 2021. The fines ranged from EUR 490 to 1,060,078 EUR. The report also shows a decrease in complaints filed with	25 August 2023	Annual Report (in Polish only)

Development	Summary	Date	Links
	the DPA – from 8318 in 2021 to 6995 in 2022. Nearly a half of these were in the private sector and concerned mostly processing of personal data in connection with the conclusion or performance of contracts. The number of breach notifications remained broadly consistent with 2021 levels. In 2021, 12,946 breaches were reported. In 2022, that number slightly decreased to 12,772 notifications. These included such matters as: incorrectly addressed correspondence; incorrect anonymization of data or inadvertent publication of data; release of data to the wrong person; loss of correspondence by the postal operator or opening of correspondence before returning it to the sender; unauthorized access to databases; paper documentation lost, stolen or left in an unsecured location; loss or theft of a data carrier; use of malicious software and interfering with the confidentiality, integrity or availability of personal data.		

Portugal

Contributors

Margarida Roda Santos
Partner

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

Paulo Sampaio Neves
Principal Associate

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

Development	Summary	Date	Links
Law no. 42/2023, 10 August 2023 which transposes the Directives (EU) 2022/211 and (EU) 2022/228 of the European Parliament and of the Council of 16 February 2023 on the protection of personal data	Law 42/2023 transposes Directives 2022/211 and 2022/228 and introduces changes to national law regarding the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and cooperation between international judicial authorities.	10 August 2023	Law no. 42/2023, August 10 (in Portuguese only)
Opinion 2023/80 on the Proposal for a Directive amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law	The National Data Protection Commission ("**CNPD**") issued an opinion regarding the proposal for a European Parliament Directive to further expand and upgrade the use of digital tools and processes in company law. CNPD concluded that the proposal only has an impact at a medium level in respect of the protection of personal data given that it is aimed at commercial companies, and states that it follows the line of thought of the European Data Protection Supervisor, and the recommendations issued on the Opinion 6/2018, on 26 July 2023 by this entity should be followed.	16 August 2023	Opinion 2023/80 (in Portuguese only)
Opinion 2023/85 regarding the draft Decree-Law amending the legal regime applicable to surrogacy	The CNPD issued an opinion on the latest version of draft Decree-Law 126/XIII/2023, which amends the legal regime applicable to surrogate pregnancies. Several recommendations are made to improve and clarify the law, including the inclusion of adequate security measures for the processing of sensitive data, as provided for in Article 9 of the GDPR.	15 September 2023	Opinion 2023/85 (in Portuguese only)

Romania

Contributors

Mihai Guia
Managing Partner

T: +40 2 13 11 25 61
mihaiguia@
eversheds-sutherland.ro

Alexandra Sulea
Partner

T: +40 21 311 2561
alexandrasulea@
eversheds-sutherland.ro

Cristian Lina
Managing Partner

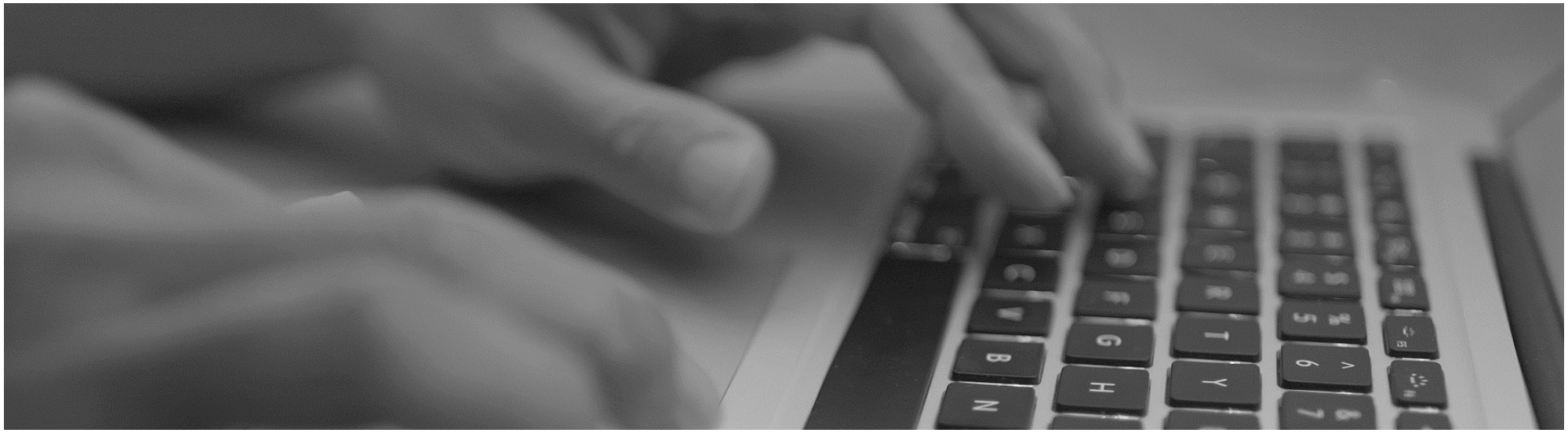
T: +40 2 13 11 25 61
cristianlina@
eversheds-sutherland.ro

Development	Summary	Date	Links
Sanction for GDPR infringement concerning the unlawful processing of personal data	The Romanian DPA concluded an investigation in August 2023 concerning a private legal entity and found violations of specific provisions of GDPR. The investigation was launched following a complaint from an individual, who reported that the controller had been sending unsolicited emails to his email address. It appears the data controller collected the personal data indirectly from public sources for the purpose of market research proposals. The investigation determined that the data controller had not provided sufficient evidence to demonstrate that it had provided clear and comprehensive information to the data subject, including information about the source of the data (as required by Article 14 GDPR). In addition, it was noted that the source of the data was not clearly presented in the privacy notice available on the data controller's website. Furthermore, it was found that the data controller failed to take the necessary measures to comply with the data subject's objection to the processing of their personal data by continuing to send a further message.	7 September 2023	Romanian DPA - Press release

Development	Summary	Date	Links
	As a result of the investigation, the Romanian DPA applied two fines, which amounted to a total of EUR 2,000 and required the data controller to take corrective measures.		
Administrative fine of EUR 2,000 issued against an individual (a physician) for taking a video with his patient and sharing it on social media without consent	During an investigation initiated following a complaint, it was discovered that the data controller, a physician, had recorded a patient at the hospital where he works using a personal phone, without the patient's consent. Subsequently, he posted the audio-video recording on his Facebook page. This audio-video recording led to the disclosure of the patient's personal data, including their image, voice, name, first name, and health status. While the data controller deleted the recording from his Facebook page on the same day, it had already been viewed by a significant number of people and had been reproduced and disseminated on various websites and mass media channels. The data controller was subject to an administrative fine in the amount of EUR 2,000 and further corrective measures imposed by the Romanian DPA.	31 August 2023	Press statement (in Romanian)
Romanian DPA applies sanctions of EUR 33,000 for cookies non-compliance and data breach	The Romanian DPA imposed two separate fines on a company in the energy sector amounting to a total of EUR 33,000, relating to non-compliance with cookies rules and a data breach. The investigation was initiated following a complaint regarding a potential breach of personal data security on the data controller's website. During the investigation, it was revealed that a file on the data controller's website containing personal data of at least 750 individuals had been publicly accessible for about two and a half years through search engine-generated links. Additionally, the data controller's website installed unnecessary technical cookies on users' devices before obtaining consent. Rejecting these cookies had no effect on their installation and the cookies remained installed on the user's device in their original form for a certain period. Corrective measures were also imposed on the company, including the implementation of a procedural plan for regular	26 September 2023	Press statement (in Romanian)

Development	Summary	Date	Links
	testing, evaluation, and assessment of systems and subsequent modifications, particularly on the operator's website.		
Romanian DPA fines software company EUR 70,000 for disclosing personal data of 600,000 users	The investigation stemmed from a data breach notification submitted by the data controller. It revealed a breach of personal data confidentiality, involving the public exposure of personal data of around 600,000 users of a software application via a publicly accessible URL. During the investigation, it was found that the data controller had not implemented adequate technical and organizational measures to prevent unauthorized access to personal data. This resulted in the unauthorized disclosure and access to personal data, including names, usernames, email addresses, employer details, country, and course-related information, for approximately ten days. As a consequence of this breach, the Romanian DPA determined that the affected individuals suffered potential physical, material, or moral harm, such as a loss of control over their personal data and a breach of data confidentiality. Considering the gravity and nature of the violation, the negligent conduct of the data controller, remedial actions taken during the investigation, and cooperation with the DPA, the data controller was fined EUR 70,000 and the DPA imposed corrective measures. The company has decided to challenge the fine and will await the final decision to be issued by the competent courts.	21 August 2023	Press statement (in Romanian)
Romanian DPA issue warning to National Consumer Protection Authority to cease the use of body cameras during their investigations into companies	In June 2023, the Romanian DPA concluded an investigation into the National Consumer Protection Authority ("**ANPC**") and identified a breach of GDPR provisions. The investigation stemmed from reports that ANPC was breaching data protection legislation by processing personal data through the use of body cameras "assigned to inspectors with control responsibilities for use in all control actions." It was reported that "for over six months, ANPC inspectors have recorded and captured, without any consent or supervision, not only colleagues, employees, or representatives of economic operators	5 July 2023	Press statement (in Romanian)

Development	Summary	Date	Links
	but also numerous private individuals, including children and adults, in stores, swimming pools, restaurants, bars, or salons." During the investigation, it was discovered that ANPC processed personal data (such as names, job titles, images, voices and behaviors) collected through body camera devices as of May 2023. The ANPC failed to provide evidence that the processing carried out with body cameras had a legal basis under applicable national law. There was no specific legal provision authorizing the use of portable audio-video recording body cameras by ANPC in relation to its specific duties.		



Singapore

Contributors

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

Teo Wen Xuan
Associate
T: +65 66 37 88 85
wenxuanteo@
gtlaw-llc.com

Phoebe Sim
Senior Associate
T: +65 66 37 88 85
phoebesim@
gtlaw-llc.com

Development	Summary	Date	Links
Personal Data Protection Commission consults on the 'Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems'	On 18 July 2023, the Personal Data Protection Commission ("**PDPC**") launched a public consultation to solicit views and comments on the Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems ("**Proposed Guidelines**"). These seek to provide clarification on how the Personal Data Protection Act 2012 ("**PDPA**") applies to the collection and use of personal data by organisations in the development and deployment of artificial intelligence ("**AI**") systems that embed machine learning models used to make decisions, recommendations or predictions. The consultation ran until 31 August 2023. The Proposed Guidelines address five key areas: **Business Improvement Exception and Research Exception** Pursuant to the PDPA, an organisation is required to obtain consent for the collection and use of personal data unless deemed consent or any exception to the consent obligation applies. The Proposed Guidelines provide some examples to demonstrate the application of the Business Improvement Exception and Research Exception where organisations are not required to obtain consent to collect or use personal data in AI systems. Where the purpose of an organisation's collection or use of personal data is to develop or enhance AI systems with the aim of improving operational efficiency by supporting decision-making,	18 July 2023	Announcement: Public Consultation for the Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems Public Consultation Proposed Advisory Guidelines on use of personal data in AI recommendation and decision systems

Development	Summary	Date	Links
	or to offer new or more personalised products and/or services, the Business Improvement Exception may be relevant. Where an organisation conducts commercial research to advance science and engineering without a product development roadmap, the Research Exception may be relevant. **Data protection considerations** The Proposed Guidelines provide guidance on the implementation of appropriate technical, process, and legal controls by organisations when using personal data to develop or enhance AI systems. **Consent and notification obligations** Organisations must comply with the consent and notification obligations under the PDPA (unless deemed consent or exceptions to the consent obligation apply), where AI systems are deployed to provide recommendations, predictions or decisions based on personal data. **Accountability obligation** Organisations that make use of AI systems should ensure that they are able to provide individuals with details on the responsible use of their personal data. Upon request, organisations should also provide individuals with information on their internal data processing policies and practices. **Procurement of AI systems** The Proposed Guidelines also set out practices for service providers who are data intermediaries to adopt. This is relevant for organisations that engage service providers who provide professional services for the development and deployment of bespoke or customisable AI systems.		
Public Consultation by Personal Data Protection Commission on the Proposed Advisory Guidelines on the PDPA for Children's Personal Data	On 19 July 2023, the Personal Data Protection Commission ("**PDPC**") launched a public consultation to solicit views and comments on the proposed Advisory Guidelines on the PDPA for Children's Personal Data ("**Proposed Guidelines (Children)**"). These seek to address issues such as obtaining children's consent, the use of children's personal data, and according higher standards of protection to children's personal data.	19 July 2023	Announcement Public Consultation

Development	Summary	Date	Links
	The Proposed Guidelines (Children) were open for public consultation until 31 August 2023.		
Undertaking by Employment and Employability Institute Pte. Ltd.	On 20 July 2023, the Personal Data Protection Commission ("**PDPC**") published a voluntary undertaking by the Employment and Employability Institute Pte. Ltd. ("**e2i**"). Key takeaways from the e2i case are as follows: – **Where more than one case involving the same organisation is being investigated, the PDPC may consider the cases together**. In this case, two separate data breaches concerning e2i were notified to the PDPC (it was alerted to the second data breach while investigating the first data breach) and the PDPC proceeded to consider both cases together. – **Organisations should ensure that their vendors, who act as data intermediaries, have reasonable security measures in place to protect personal data**. In this case, the PDPC accepted e2i's undertaking on the basis that notwithstanding e2i's failure to stipulate personal data protection requirements in its contract with the vendor, e2i had engaged the vendor on account of the vendor's good personal data protection policies and processes. – **In deciding whether to accept an undertaking, the PDPC may also consider whether there is any evidence of unauthorised access to the personal data or data exfiltration**. In this case, it appears that the PDPC accepted e2i's undertaking as there was no evidence suggesting that there had been unauthorised access or data exfiltration; this is consistent with the PDPC's practice with respect to other personal data breaches similar to the one that affected e2i's website.	20 July 2023	Undertaking to PDPC
Updates to the advisory guidelines on the application of the Personal Data Protection Act to election activities	On 28 July 2023, the Advisory Guidelines on the Application of the Personal Data Protection Act to Election Activities ("**Advisory Guidelines (Election Activities)**") were updated to provide further clarity on the amendments to the Personal Data Protection Act 2012 ("**PDPA**") which came into force on 1 February 2021, and in view of the then-upcoming Singapore presidential election on 1 September 2023.	28 July 2023	Advisory Guidelines

Development	Summary	Date	Links
	The Advisory Guidelines (Election Activities) highlight how key provisions of the PDPA apply to political parties and election candidates when carrying out election activities.		
Publication of advisory on cybersecurity for elections in Singapore	On 31 July 2023, the Elections Department Singapore issued an advisory to election candidates and political parties, which was aimed at mitigating the risk of cyber incidents disrupting their activities by providing information on potential cyber threats and the preventive measures to be taken in response.	31 July 2023	Advisory on Cybersecurity for Elections in Singapore

Enforcement decision for breach of the protection obligation	In this enforcement decision, an e-commerce business was fined S$74,400 by the Personal Data Protection Commission ("**PDPC**") for failing to put in place reasonable security arrangements to protect users' personal data in its possession or under its control, in breach of section 24 of the PDPA (the "**Protection Obligation**"). The data breach incident had occurred when a hacker gained unauthorised access to the business's customer data servers.
	
	Key takeaways from the case are as follows:
	– The business was determined to have breached the Protection Obligation in two respects:
	  – a lack of sufficiently robust processes for certain vendor web servies key management; and
	  – a failure to conduct periodic security reviews.
	– The PDPC highlighted that organisations cannot place sole reliance on their employees to perform their duties properly as a security arrangement to protect personal data. There must be some processes implemented to ensure that the step required from the employee is taken, such as independent verification by another checker.
	– An aggravating factor, which the PDPC took into account when determining whether to impose a financial penalty and the amount of such penalty, was that the business took 15 days to respond to the compromise of customer data. This was indicative of a lack of sufficiently robust processes to monitor its incident management response to ensure reasonable remediation speed.
		16 August 2023	Press Release

Development	Summary	Date	Links
Singapore Cyber Security Agency and Dragos, Inc sign memorandum of understanding to strengthen Singapore's capabilities in operational technology cybersecurity	On 22 August 2023, the Cyber Security Agency of Singapore ("**CSA**") signed a 3-year Memorandum of Understanding ("**MOU**") with Dragos, Inc. at the Operational Technology Cybersecurity Expert Panel Forum 2023. The MOU addresses information-sharing, capacity, and capability-building for Operational Technology cybersecurity to enable Singapore to defend against cyber-attacks, and will also support CSA's efforts in enhancing Singapore's national cyber defence capabilities by leveraging Dragos Platform technology. The areas of collaboration will cover the following: – Threat intelligence – Consultancy and risk assessment – Incident response – Information exchange and training	22 August 2023	Press Release
Smart Nation and Digital Government Group and Ministry of Communications and Information to merge from October 2023	From 23 October 2023, the Smart Nation and Digital Government Group is merging with the Ministry of Communications and Information ("**MCI**")'s digital development functions to form an enlarged Smart Nation group. The merger will take effect in phases, with MCI commencing the administration of the Smart Nation group from 23 October 2023.	12 September 2023	Press Release
Singapore and New Zealand sign Memorandum of Arrangement for enhanced cooperation on scam and spam communications	The Infocomm Media Development Authority and New Zealand Department of Internal Affairs ("**DIA**") have signed a Memorandum of Arrangement ("**MOA**") for enhanced cooperation between both countries to combat scam and spam communications. The MOA seeks to strengthen collaboration in projects aimed at enhancing anti-scam measures and strengthening information exchanges between both countries on scam trends, regulatory and technological solutions and public education.	14 September 2023	Press Release

South Africa

Contributors

Grant Williams
Partner

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

Development	Summary	Date	Links
Information Regulator receives a proposed code of conduct from Residential Communities Council on how personal information will be processed in the Residential Community Industry	On 8 September 2023, the Information Regulator published a notice (dated 25 August 2023) in the Government Gazette stating that it had received a proposed code of conduct from the Residential Communities Council ("**RCC**") dealing with how personal information will be processed in the Residential Community Industry ("**RCI**"). This has recently become a topic of discussion, as many residential communities and estates require visitors to provide their personal data when entering the estate. It is not clear what happens to that personal data, and how it is processed or stored. The purpose of the code of conduct is to: – Promote appropriate practices by members of RCC governing the processing of personal information in terms of POPIA; – Encourage the establishment of appropriate agreements between members of RCC and third parties, regulating the processing of personal information as required by POPIA and dictated by good business practice; and – Establish procedures for members of RCC to be guided in their interpretation of POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against RCC to be considered and remedial action, where appropriate, to be taken. Affected persons were invited to submit written comments to the Information Regulator email address: POPIACompliance@inforegulator.org.za within 14 days after publication of the notice in the Government Gazette.	8 September 2023	Proposed Code of Conduct Residential Communities Council

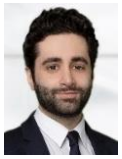
Development	Summary	Date	Links
Enforcement notice issued to major pharmaceutical company for contravention of POPIA	On 31 August 2023, the Information Regulator issued an Enforcement Notice to a major pharmaceutical company following a finding of the contravention of various sections of the Protection of Personal Information Act ("**POPIA**"). In terms of the Enforcement Notice, the company must: – Conduct a Personal Information Impact Assessment. – Implement an adequate Incident Response Plan. – Implement the Payment Card Industry Data Security Standards. – Ensure that it concludes written contracts with all operators who process personal information on its behalf, and that such contracts compel the operator(s) to establish and maintain same or better security measures referred to in section 19 POPIA. – Develop, implement, monitor, and maintain a compliance framework, in terms of Regulation 4(1)(a) POPIA which clearly makes provision for the reporting obligations of The Company and all its operators in terms of section 22 of POPIA. – The company must provide a report to the Information Regulator on the implementation of the actions ordered in the Enforcement Notice within thirty-one (31) days of the issuing and receipt. Should the company fail to abide by the Enforcement Notice within the stipulated timeframe, it will be guilty of an offence, on which the Regulator may impose an administrative fine of an amount not exceeding R10 million or be liable upon conviction to imprisonment or both.	1 September 2023	Information Regulator Media Statement - Enforcement Notice issued to Dis-Chem
Infringement notice and R5 Million administrative fine issued to Department of Justice and Constitutional Development for Contravention of POPIA	On 3 July 2023, the Information Regulator issued an Infringement Notice to the Department of Justice and Constitutional Development in which it ordered payment of an administrative fine of R5 million following its failure to comply with the Enforcement Notice issued by the Information Regulator on 9 May 2023.	4 July 2023	Media Statement - Infringement notice and fine issued to Department of Justice and Constitutional Development

Development	Summary	Date	Links
	The Information Regulator issued the Enforcement Notice after finding a contravention of various sections of the Protection of Personal Information Act (POPIA) by the Department. The Enforcement Notice had required the Department to submit proof to the Information Regulator within thirty one (31) days of receipt of the Enforcement Notice that the Trend Anti-Virus licence, the SIEM licence and the Intrusion Detection System licence have been renewed. It also required the Department to initiate disciplinary proceedings against the official/s who failed to renew the licences, which are necessary to safeguard the department against security compromises. As the Department did not provide the Information Regulator with the required report / proof, the Information Regulator has made a determination that the Department failed to comply with the Enforcement Notice. Accordingly, the Regulator has issued an administrative fine of R5 million to the department for failure to comply with the Enforcement Notice. The Department was given 30 days, from 3 July 2023, to pay the administrative fine or make arrangements with the Information Regulator to pay the administrative fine in instalments or elect to be tried in court on a charge of having committed the alleged offence referred in terms of POPIA.		

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
Digital learning platform for Swedish schools issued with reprimand for API exploit	The Swedish DPA issued a reprimand against a company that provides a digital learning platform for several schools in Sweden. The platform is mainly used for communication between students, parents and teachers A student that belonged to one of the schools that was using the platform exploited a vulnerability in the platform's API call function for address books and managed to extract personal data regarding other students from various schools. The extracted data, which included names, pictures, e-mail addresses and telephone numbers, was then published on a website. The responsible company was first made aware of the incident after a student had informed them of the website where the extracted data was published. The incident also resulted in over 60 reports of personal data breaches being sent to the Swedish DPA. The Swedish DPA concluded that the responsible company lacked appropriate systems to monitor API calls made to the platform's address books. Had a monitoring system been implemented, the responsible company would have been able to detect discrepancies and identify the unlawfully extracted data. However, the Swedish DPA also recognised that the platform included access control and a monitoring system for other parts of the platform. Furthermore, the extracted personal data did not include any sensitive personal data Based on these findings, the Swedish DPA opted to issue only a reprimand for the incident.	25 August 2023	Press statement (in Swedish) Decision (in Swedish)

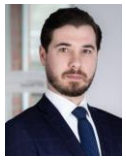
Development	Summary	Date	Links
Major Swedish insurance provider receives administrative fine of SEK 35 million for security flaw	The Swedish DPA issued an administrative fine of SEK 35 million to a major Swedish insurance provider for failing to protect sensitive personal data of customers. After receiving a tip, the Swedish DPA initiated an audit of the insurance company. The person who contacted the Swedish DPA had received an email from the company with a link to a web page with price quotes. On this web page, there were clickable links with URLs that led to documents with insurance information. However, the person noticed that it was possible to access other insurance policyholders' documents, without any kind of login or access control, by simply replacing a few numbers in the web link. The audit revealed that it was possible via this exploit to access data belonging to over 650,000 customers. The customer data included information on health and financial status, contact details, social security numbers and insurance holdings. Certain documents also contained more detailed information on the customers' health status. The Swedish DPA concluded that the deficiencies were of such a fundamental nature that the insurance provider should have had the opportunity to discover and remedy these even before the relevant IT system was introduced and in any case during the long period that the system was used. Another interesting point in the decision was that the Swedish DPA considers that the processing of personal data is part of an insurance provider's core business.	30 August 2023	Press statement (in English) Decision (in Swedish)
Swedish DPA establishes accreditation requirements for monitoring bodies	Pursuant to article 40(1) GDPR, supervisory authorities shall encourage the drawing up of codes of conduct intended to contribute to the proper application of GDPR. To this end, the Swedish DPA will establish accreditation requirements for monitoring bodies. In Sweden, certain trade associations that have already established ethical guidelines relating to data protection. For example, members of the Swedish Data & Marketing Association ("**SWEDMA**") are expected to follow the association's ethical	7 September 2023	Press statement (in Swedish) Decision (in Swedish)

Development	Summary	Date	Links
	guidelines on data privacy when advertising their services or products. It remains to be seen whether SWEDMA or similar trade associations in Sweden will begin the process of drawing up codes of conduct relating to GDPR now that the accreditation requirements for monitoring bodies have been formally established by the Swedish DPA.		
Revised exemptions list regarding processing criminal data proposed by Swedish DPA	As previously reported in Updata Edition 18, the Swedish DPA concluded that data controllers who must assess customer risk profiles pursuant to the Swedish Anti-Money Laundering Act (2017:630) are not allowed on this basis alone to process personal data relating to criminal convictions and offences ("**criminal data**"). In other words, Swedish banks and other financial institutions must receive permission from the Swedish DPA prior to processing criminal data. This also includes screening customers against sanctions lists. Due to the above decision, the number of applications made by financial institutions seeking permission to process criminal data has increased substantially. The Swedish DPA now believes that too many resources are being spent on managing these applications and have therefore proposed to expand the list of processing operations that are exempted from the relevant requirement. One exemption includes banks and other financial institutions that want to check sanctions lists for the purpose of complying with the Swedish Anti-Money Laundering Act.	18 September 2023	Press statement (in Swedish) Proposal (in Swedish)

Switzerland

Contributors

Markus Näf
Partner
T: +41 58 255 56 50
markus.naef@
eversheds-sutherland.ch



Leonid Shmatenko
Senior Associate
M: + 41 76 782 99 75
leonid.shmatenko@
eversheds-sutherland.ch

Timon Meindl
Trainee

Carol Tissot
Legal Director
T: +41 58 255 57 00
carol.tissot@
eversheds-sutherland.ch

Oliver Scharp
Associate
oliver.scharp@
eversheds-sutherland.ch

Development	Summary	Date	Links
New Data Protection Act (FADP) and related laws and ordinances been in force from 1 September 2023 without transitional provisions	The completely revised Data Protection Act and the implementing provisions in the new Data Protection Ordinance and the new Ordinance on Data Protection Certifications have been in force since 1 September 2023. The most important changes include the following: – Companies must clearly communicate what rights and options data subjects have. In addition, companies must provide clear information about the collection, storage, processing, and use of the data, as well as take measures according to the person's data protection preferences – The new FADP makes it easier for data subjects to exercise their right to information. This is because they do not have to disclose personal data or information about how they are connected to the person who processed their data. Any person can request details of the personal data collected and stored about them. – Violations of the new provisions can lead to fines of up to CHF 250,000 for private individuals. In contrast to the GDPR, only intentional acts and omissions, such as disregarding information and violating due diligence obligations, are	1 September 2023	Revised Data Protection Act

Development	Summary	Date	Links
	punishable. In principle, only the individual responsible is fined. However, the company itself can also be fined up to CHF 50,000 if the identification of the offending natural person within the company would require a disproportionate effort. – Current data protection and processing principles must already be incorporated into the planning and design of applications for user privacy to be taken into account. In this way, companies develop applications according to the "security first" principle instead of improving the security features afterwards or even after an incident.		
FDPIC launches online reporting portal for data security breaches in light of FADP	The FDPIC provides those responsible with an online form where reports can be submitted in a secure and digital manner. After submitting the report, the persons responsible can download a confirmation containing the reported information Only breaches of data security that lead to the unintentional or unlawful loss, deletion, destruction or alteration of personal data, or to its disclosure or access by unauthorised persons, and which are likely to result in a high risk to the personal or fundamental rights of data subjects, must be reported to the FDPIC.	1 September 2023	Reporting Portal
FDPIC publishes information sheet on data protection impact assessments	The FDPIC's information sheet is primarily aimed at private data processors, although it can also be consulted by federal bodies as an aid to interpretation. The information sheet provides an overview of the subject matter, purposes and objects of protection for the data protection impact assessment ("**DPIA**"). The purpose of the DPIA is to identify, assess and deal with data protection risks and is not limited to the foreseeability and assessment of "high" project risks. One practical benefit of the information sheet is the commentary on systemic and security-related risks and reduction of these risks to a level acceptable under data protection law by means of suitable measures Furthermore, interpretation aids for the characterisation of "high risk" are provided. Likewise, the risk pre-audit and the obligation to carry out the DPIA are explained. The information sheet alsio provides support for the preparation of the DPIA.	31 August 2023	FDPIC - Basics of the data protection impact assessment FDPIC - Information sheet on data protection impact assessment

Development	Summary	Date	Links
New obligation for foreign officers to appoint a representative in Switzerland	Private controllers with their registered office or place of residence abroad who process data on individuals in Switzerland must designate a representation in Switzerland if the following cumulative requirements are met: – Offering of goods or services in Switzerland or behavioural monitoring; – Extensive processing; – Regular processing; and – High risk to the personality of the person concerned. The representative acts as a point of contact for the data subject and the FDPIC. The data controller only has to publish the name and address of the representative in Switzerland, e.g. on their website. The representative has the following minimum obligations: – Keeping a register of data processing activities; and – Reporting and information obligations vis-à-vis the FDPIC and data subjects. However, the representative is not the contact person for criminal proceedings. These must be served directly to the controller.	1 September 2023	Revised Data Protection Act

United Kingdom

Contributors

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

Liz Fitzsimons
Partner
T: +44 1223 44 3808
lizfitzsimons@
eversheds-sutherland.com

Dave Hughes
Partner
T: +44 1223 44 3642
davidlhughes@
eversheds-sutherland.com

Philip James
Partner
T: +44 20 7919 0700
philipjames@
eversheds-sutherland.com

Gayle McFarlane
Partner
T: +44 121 232 1262
gaylemcfarlane@
eversheds-sutherland.com

Development	Summary	Date	Links
UK and Singapore sign memorandum of understanding agreements to advance research and regulatory cooperation	On his first international visit since his appointment last year, the UK's Deputy Prime Minister, Oliver Dowden signed two agreements with Singapore's Minister for Communications and Information, building on the 2022 UK-Singapore Digital Economy Agreement and the 2020 UK-Singapore Free Trade Agreement.	28 June 2023	Press release
AI assurance case studies	The Centre for Data Ethics and Innovation and Department for Science, Innovation and Technology published a series of case studies to assist organisations in using AI assurance techniques to comply with the principles set out in the AI White Paper.	7 June 2023	Press release Case study portfolio
UK granted Associate status in Global Cross Border Privacy Rules Forum	The Global Cross Border Privacy Rules ("**CBPR**") Forum granted the UK 'Associate' status.	3 June 2023	UK press release Global CBPR Forum press release

Development	Summary	Date	Links
	The CBPR Forum works to support international data transfers between its member countries – Australia, Canada, Japan, Republic of Korea, Mexico, Philippines, Singapore, Chinese Taipei and the United States. The relevant criteria for participating in the Forum is that the applicant: (a) supports the principles and objectives of the Forum provided in the 2022 Global CBPR Declaration and the Global CBPR Framework; (b) has law(s) and/or regulation(s), the enforcement of which has the effect of protecting personal information; and (c) has at least one public body that is responsible for enforcing law(s) and/or regulation(s) within the meaning of item (b) and has the powers to conduct investigations or pursue enforcement proceedings. In considering the UK's application, the CBPR Forum's Membership Committee undertook consultations with representatives of the UK Department for Science, Innovation and Technology to clarify elements of the UK's application.		
ICO submits its journalism code of practice to the Secretary of State.	The Information Commissioner's Office ("**ICO**") submitted its draft code of practice on the use of personal data for journalism (the "**Code**") to the Secretary of State at the Department of Science Innovation and Technology, for approval, before laying it before Parliament. Provided there are no objections, the Code will likely come into force in the coming months. The Code provides guidance and clarification on case law and legislation applicable to the use of personal information in the field of journalism, including detail on the specific GDPR journalism exemption and on how individuals can complain or seek to exercise their rights over their personal data processed by journalists. The Code is currently with the Secretary of State for the Department for Science, Innovation and Technology, who will present it to Parliament.	6 July 2023	ICO submits Data protection and journalism code of practice to the Secretary of State
UK announces first law enforcement adequacy decision to the Bailiwick of Guernsey	The UK announced its first law enforcement data adequacy decision with Bailiwick of Guernsey. This decision enables personal data from law enforcement authorities to be freely transferred from between UK and the Bailiwick of Guernsey authorities without the need for additional safeguards.	7 July 2023	UK finalises first law enforcement data adequacy decision

Development	Summary	Date	Links
	This is the first law enforcement data adequacy decision made by the UK government since leaving the EU. An adequacy decision is when the government determines that that another jurisdiction has the necessary data privacy safeguards in place to protect UK personal data. It is expected that the Isle of Man will also receive an adequacy decision in the near future. As the UK government press release states, it should be noted that for both the Bailiwick of Guernsey and the Isle of Man, "the UK already recognises both jurisdictions' EU adequacy decision for UK GDPR purposes."		
New Internet of Things legislation laid before Parliament	The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 were laid before Parliament on 10 July 2023, and reached their final form wording on 14 September 2023. The Regulations set out the minimum cyber security requirements with which internet or network connectable ("smart") products made available to consumers in the UK will have to comply from 29 April 2024. The Regulations 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. They will require manufacturers of in-scope products to: – use unique, rather than universal, default passwords for products. Unique passwords must not be based on incremental counters, derived from publicly available information or unique product identifiers or be otherwise guessable – publish information on a point of contact for consumers to report security issues relating to products and details of when status updates on resolution of reported security issues will be given – publish details of the minimum period during which products will receive security updates, including as part of the	10 July 2023	Statutory Instrument page The Product Security and Telecommunications (Security Requirements for Relevant Connectable Products) Regulations 2023

Development	Summary	Date	Links
	consumer protection law pre-contract information provided on websites advertising the products for sale Information must be accessible, clear and transparent and made available to consumers in English, free of charge, without request and without a requirement for provision of personal data. The definition of products for these purposes includes hardware, pre-installed software, software that has to be installed on the product and, for the reporting of security issues and security update provisions, software associated with the product's intended functionality, which could include cloud services or "companion apps". Where there are multiple manufacturers of a product, each of them has to comply with these rules. The explanatory memorandum to the Regulations explains that this is intended to ensure that where white label products are sold under a business's brand, that business as well as the original manufacturer will have to comply. 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. 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 (but not computers designed exclusively for under 14s which remain in-scope). Businesses that manufacture, import or distribute consumer connectable products should be putting in place measures to ensure that they are ready to comply with the new rules when they come into force.		

Development	Summary	Date	Links
ICO and FCA seek to clarify position on Consumer Duty / direct marketing rules interplay	In a joint letter to UK Finance and the Building Societies Association, the Financial Conduct Authority ("**FCA**") and Information Commissioner's Office ("**ICO**") clarified that data protection rules around sending direct marketing communications do not prevent firms from informing their savings customers about better deals. The letter, published against a backdrop of ever increasing cost of living pressures, seeks to address confusion that emerged amid recent discussions between financial firms and the FCA and ICO in relation to obligations under the new Consumer Duty. The duty requires firms to "'act to deliver good outcomes for retail customers", and in doing so ensure customers are provided with the information they need, at the right time, and presented in a way they can understand. The letter confirms that the UK GDPR's right to object to direct marketing does not prohibit firms from providing communications to their customers when requested or required by a statutory regulator, such as the Consumer Duty. In practice: *Firms can provide regulatory communications to all their savings customers that provide neutral, factual information about the interest rate and terms of the savings product they hold, the interest rate and terms of other available savings products, and what their options are for moving to another product.* *There are also other approaches available to firms which could be adopted to engage their customers and support effective decision making, such as displaying the regulatory communication on their website.* Although this update specifically relates to financial sector, the underlying message is applicable to all organisations looking to reconcile their direct marketing communications strategies with their statutory regulatory obligations. The ICO has issued guidance on direct marketing and regulatory communications to help.	18 July 2023	Joint letter from the ICO and FCA to UK Finance and Building Societies Association ICO guidance on direct marketing and regulatory communications

Development	Summary	Date	Links
House of Lords Library report on AI	The House of Lords Library published a report on AI: development, risks and regulation. This provides a comprehensive overview on what AI is, risks and benefits, potential impacts, what the UK regulatory landscape looks like and how it compares to other countries.	18 July 2023	Artificial intelligence: Development, risks and regulation
AI Council to be replaced by expert group	The UK AI Council published an update, explaining that the terms of the current members are coming to an end and that the Department for Science, Innovation and Technology will be replacing the Council with a wider group of expert advisers to input on a variety of priority issues including AI.	7 July 2023	AI Council
Inquiry into large language models (generative AI)	The House of Lords Communications and Digital Committee carried out an inquiry into large language models, which it describes as "a type of generative AI which have attracted significant interest for their ability to produce human-like text, code and translations". The purpose of the inquiry is to consider the potential benefits and risks of large language models, in particular to consider what needs to happen in the next 1 to 3 years to ensure that the UK is in the best position to respond to both opportunities and risks. Risks and unknowns identified by the Committee include generation of incorrect information, use of biased or harmful information, promotion of disinformation and fraud, uncertain IPR ownership and lack of transparency in decision-making. As part of this inquiry the Committee launched a call for written evidence, which includes questions on how adequately the UK Government's AI White Paper deals with large language models and whether a tailored regulatory approach is required, and how the UK's approach compares to that of other nations. Contributions were required by 5 September. Developers and users of AI alike should consider responding to this in order to contribute to the debate that is shaping policy in this area.	7 July 2023	Large language models - Committees - UK Parliament
Proposed online fraud charter for the tech sector	The Government published an update on the latest meeting of the Joint Fraud Taskforce, at which the UK fraud strategy launched in May was discussed. The aim of the strategy is to reduce fraud by 10% from 2019 levels by 2025.	11 July 2023	Government and industry meet to progress the fight against fraud

Development	Summary	Date	Links
	The strategy is particularly focussed on measures to reduce online scams and fraud, and the latest update reports progress on development of an online fraud charter for the tech sector. According to the update "The charter will ensure that tech firms take action to block scams, make it easier to report frauds and ensure that fraudulent content is removed swiftly". The Security Minister has also "called on tech firms to implement stronger measures to tackle fraud on their platforms ahead of the introduction of the Online Safety Bill". The update also reports that the Joint Fraud Taskforce discussed a proposed anti-fraud public awareness campaign to "streamline and simplify messaging to the public". Businesses in the tech sector should monitor development of the online fraud charter and consider measures they can take to reduce fraud on their platforms.		
ICO statement on banks sharing and gathering personal data	Following the recent (and high profile) Nigel Farage complaint in respect of the closure of his Coutts bank account (and significant coverage of this in the media), which had involved Farage obtaining information about this through a data subject access request, the Information Commissioner released a brief statement addressed to banks about their data protection responsibilities. The statement makes clear that, somewhat unsurprisingly, the banking duty of confidentiality "would not permit the discussion of a customer's personal information with the media". The Information Commissioner further states that "Banks should not be holding inaccurate information, they should not be using information in a way that is unduly unexpected, and they should not be holding any more information than is necessary. Even the information banks gather around politically exposed persons must follow the law" and that the ICO is working with the HM Treasury and the FCA on this (politically exposed persons). The Information Commissioner used the Farage case to highlight why the individual data subject right to access personal data under UK GDPR is such an important right.	26 July 2023	Statement

Development	Summary	Date	Links
	It remains to be seen whether banks (or other organisations) receive an increased number of data subject access rights following the media coverage of this matter.		
ICO updates guidance on whether internet-based services are likely to be accessed" by children (and therefore within the scope of the Children's code)	For background, the ICO's Children's code (*Age appropriate design: a code of practice for online services*) applies to providers of internet services (defined as information society services) which are "likely to be accessed by children", even if they are not designed or intended for children's use. Following its consultation earlier this year, the ICO updated its FAQ guidance on whether services are "likely" to be accessed by children (and therefore fall within the scope of the code even if not intended to be accessed by children). Providers of internet services who, having considered the factors set out in the guidance, determine that their services are not likely to be accessed by children (and hence do not have to comply with the code), should revise their view if there is subsequent evidence that a "significant number" of children are in fact accessing the service. The guidance does not set a figure on the level of numbers that are "significant", although it makes clear that the threshold is potentially low (ie "more than de-minimis or insignificant") and that the greater the risks are to the children, the lower the threshold will be. Where a service is not intended to be accessed by children but nevertheless children are likely to access the service, the provider can: – comply with the code in a proportionate way; or – apply age-gating to prevent children from accessing the service in the first place, meaning that they are no longer likely to access it (and therefore the code will not apply) The guidance contains relevant case studies/examples, including (amongst others) online dating and hobbies websites.		Children's Code Guidance

Development	Summary	Date	Links
House of Lords letter to Government on Digital Markets, Competition and Consumers Bill	The House of Lords has released a letter sent by its Communications and Digital Committee to the Secretary of State for Business and Trade, containing a number of recommendations in relation to the Digital Markets, Competition and Consumers Bill. The letter follows the Committee's call for evidence in May 2023, on Parts 1 and 2 of the Bill which deal with digital markets and competition. The Committee has concluded that the Bill's aims are sound and its measures are "broadly proportionate". In its letter, the Committee states: – its support for the Bill's objectives by confirming that the "need for pro-competition legislation to improve digital competition is clear" – that the judicial review standard is appropriate and must be maintained. It calls on the Government to resist any move towards a full merits appeal, including a time-limited full merits appeal, as sought by big tech firms – the countervailing benefits exemption (allowing a firm accused of breaching a conduct requirement a defence where its actions provide a sufficient consumer benefit) provides a proportionate backstop as long as the threshold for relying on it remains high, and that the Government must resist changes that would lower the threshold – the leveraging principle (that allows conduct that is for the purpose of preventing a designated undertaking from carrying on activities other than the relevant digital activity in a way that is likely to bolster the strategic significance of its position, in relation to the relevant digital activity) is a proportionate measure and should be retained in its current form – and that the CMA should provide detailed guidance on the issue – a well-resourced competition regulator should not be under estimated, and that the Treasury should keep the Digital Market Unit ("DMU")'s resourcing under review – the DMU will need to "*hit the ground running*" to keep pace with other jurisdictions' efforts in this area	21 July 2023	

Development	Summary	Date	Links
	– transparency will be key to maintaining public confidence in the CMA's work, and the CMA should be proactive in ensuring its new powers are accompanied by stakeholder communications and transparent accountability processes Clients should continue to follow the Bill's progress as it passes through Parliament. At the time of writing, the Bill is due to have its report stage and third reading on a date to be announced.		
ICO and CMA denounce misleading and harmful website design and cookie practices	The ICO and Competition and Markets Authority ("**CMA**") have called for an end to harmful website designs and practices that can mislead individuals into reluctantly providing superfluous personal information online and distort consumer choice. As part of their work within the Digital Regulation Cooperation Forum, the two regulators have published a position paper, highlighting a number of problematic practices, namely: "harmful nudges and sludge", "confirmshaming", "biased framing", "bundled consent" and "default settings" and illustrating how such practices can be detrimental to individuals. The paper also sets out key questions that firms should consider when seeking to engage users about how their personal data is processed online, to support good practice and drive pro-privacy and pro-competition outcomes in digital markets. The ICO and CMA will be supporting individuals, including educating and encouraging them to report "sneaky online sales tactics". The ICO will also be "assessing cookie banners of the most frequently used websites in the UK, and taking action where harmful design is affecting consumers". The ICO simultaneously published a blog post aimed at organisations commissioning websites, web designers and developers which reinforces the position paper's message – in particular to configure online choice to build customer trust, by: – putting the user at the heart of design choices; – using design that empowers user choice and control; – testing and trialling design choices; and – complying with data protection, consumer and competition law.	9 August 2023	ICO and CMA: Harmful online design encourages consumers to hand over personal information It's time to end damaging website design practices that may harm your users ICO-CMA joint paper on Harmful Design in Digital Markets Harmful Design in-Digital Markets

Development	Summary	Date	Links
	The regulators' comments align with their wider warnings against the use of nudge tactics and dark patterns for online sales and marketing purposes, specifically the "ICO's Age appropriate design" code of practice and the CMA's work in relation to online choice architecture and its "Rip-off Tip-off" campaign. This development has also emerged against a backdrop of increased regulatory scrutiny of and enforcement against the improper use of online advertising technologies globally. Organisations should review their website practices in light of these latest remarks. Eversheds Sutherland's international Privacy, Competition and Consumer law specialists are able to help clients navigate and address these complex issues, please do not hesitate to get in touch.		
Connected tech: smart or sinister? UK Government report	The UK Culture Media and Sport Committee has called for more to be done to protect privacy rights and young people in the launch of its report into Connected tech: smart or sinister? The report follows an inquiry into the use of connected devices and the predicted increase in the use of "smart environments" in everyday life looking at the benefits and risks posed. Key findings and recommendations cover the topics of data and privacy, product security and tech abuse and include: – measures should be introduced to standardise privacy interfaces for connected devices – these should be clear and easily digestible by the user so they understand how their personal data is being collated – the Online Safety Bill should ensure that "voice assistants", connected devices like smart speakers and other emerging tech fall within its requirements (especially those that link to search engines) – the ICO should assist in ensuring connected tech in schools and homes contains age-appropriate terms and conditions so children's privacy is not compromised – monitoring of employees in smart workplaces to only be done with the consent of those employees. The ICO is called to develop its current guidance into a code of practice	7 August 2023	Connected tech: smart or sinister?

Development	Summary	Date	Links

	– strengthening product security by promoting the guidelines not included in the Product Security and Telecommunications Infrastructure Act 2022 and codifying these remaining guidelines in phases in order to "stay ahead of emerging cyber threats"
	– more is required to address the skills shortage in the cyber security sector
	– tackling "tech abuse" should be a priority with:
	  – "upskilling law enforcement to improve the criminal justice response and increasing law enforcement's and victims' and survivors' awareness of specialist services"
	  – the Office for Product Safety and Standards (OPSS) to convene a working group to "bring industry together" so that products are designed to mitigate the risk of abuse and awareness is raised on this issue
	A second Committee report is due later this year focussing on the impact of connected tech and AI and on the creative industries.		

ICO publishes draft guidance (for consultation) on biometric data	For background, the ICO is taking a 2-phased approach to producing guidance on biometric data and the use of biometric technologies. The first phase covers (draft) guidance on how data protection law applies when using biometric data in biometric recognition systems, and has been published for public consultation. The second phase will follow and will cover biometric classification and data protection, including a call for public evidence in 2024. The guidance is aimed at users and vendors of biometric recognition systems (eg facial, voice or fingerprint recognition, keystroke analysis, gaze analysis, amongst others) – and is relevant to both controllers and processors.	18 August 2023	ICO consultation on the draft biometric data guidance

Development	Summary	Date	Links
	The guidance makes clear that whether personal data constitutes "biometric data" depends on the qualities/features of the data itself, rather than how it is used – but in order for it to be additionally classified as "special category personal data" (under Article 9 UK GDPR) it must be used for unique identification. Special category personal data is deemed higher risk under UK GDPR and therefore its processing requires additional safeguards. Reflecting terms defined by industry standards rather than set out in the UK GDPR, "biometric recognition" in the context of the guidance refers to the use of biometric data for the purposes of: – identification (ie a one-to-many matching process), or – verification (ie a one-to-one matching process) Organisations using a biometric recognition system are, by default, processing biometric data – because the information created by the use of the recognition system: – is about someone's physical, psychological or behavioural characteristics – results from processing which allows the unique identification of someone (eg through creating a biometric sample and/or template) – allows or confirms unique identification (ie it is possible to do this from the information created by the system, even if the organisation doesn't intend to be able to uniquely identify someone) It follows that biometric data processed in this way will constitute special category personal data – because at least at some stage of the process (even if it isn't the organisation's ultimate aim) there is the purpose of uniquely identifying someone from the biometric data processed.		

Development	Summary	Date	Links
	The guidance further states that use of a biometric recognition system is "highly likely" to trigger requirements under the UK GDPR to carry out a data protection impact assessment ("DPIA"), and that in most cases explicit consent of the individual to whom the data relates will be the only lawful basis available for processing the biometric data (and that organisations must offer a suitable alternative to people who choose not to consent). It also reminds organisations that use of biometric recognition systems may in many cases involve the making of solely automated decisions which have legal or similarly significant effect on individuals (and therefore require further safeguards under UK GDPR including providing the right to request human review of the automated decisions taken). In terms of appropriate security measures to protect biometric data, the guidance states that biometric data "must be encrypted". Finally, the guidance discusses the accuracy risks associated with biometric recognition systems (ie probability-based matching results in the potential for false positives and false negatives) and the risks of discrimination. The consultation period ended on 20 October 2023.		
House of Commons research paper on AI and employment law	The House of Commons Library has published a research briefing on *Artificial intelligence and employment law* which provides a helpful overview of the legal issues relating to the deployment of AI in an employment context. The briefing sets out a number of illustrative examples of AI being deployed as a workplace tool in three broad areas: recruitment, line management, and monitoring & surveillance. The example scenarios are taken from the UK, Europe, the US and China. The briefing also explores the current UK laws affecting the use of AI and employment – including the relationship between employer and employee under common law, relevant laws concerning equality and fairness, the right to privacy enshrined in the European Convention on Human Rights and data protection laws.	11 August 2023	Artificial intelligence and employment law

Development	Summary	Date	Links
	The paper discusses the ongoing development of policy and regulation as it relates to AI and employment. The relevant sections summarise the UK Government's proposed approach (highlighting its principles-based and non-statutory framework), as well as the alternative proposals that have been suggested by other bodies such as the All-Party Parliamentary Group and Trades Union Congress. Finally, the paper briefly outlines the regulation efforts in respect of AI and employment at EU level and in the US. The paper is a useful and accessible resource for clients seeking an introduction to the laws governing and impacting the use of AI in an employment context		
New ICO guidance on sending bulk emails	The ICO has published guidance (and an accompanying blog post) on what organisations must, should and could do when sending bulk emails in order to comply with data protection laws. Regardless of the nature of the information within the body of the email, identifying the recipient(s) or those CC'd or BCC'd within an email may reveal sensitive information about the individual by allowing others to identify the person, which means that such information should be treated as special category personal information and a higher level of protection afforded to its transmission. The guidance also contains a number of case studies illustrating how misuse of bulk email can compromise security of personal data. The guidance then goes on to outline what controllers *must* and *should* do in relation to sending bulk emails. Controllers must: – consider using alternative secure methods (beyond CC and BCC) such as bulk email services or mail merge services, where there is a risk that revealing the identity of the recipients may reveal sensitive personal information to other users – assess which technical and organisational security measures are appropriate in the circumstances to protect personal	30 August 2023	Guidance Blog post

Development	Summary	Date	Links
	information (such as using alternative bulk email sharing services) – ascertain who will be viewing/sending the information (such as any third party) and whether they are a processor/controller, ensuring that any third party sending emails on your behalf remain compliant as if it was an email sent on their own behalf – take a risk based approach when determining whether to implement methods for sharing bulk emails, where sending sensitive personal information, BCC should not be used. Cost implications can be considered when planning – report breaches arising from non-compliant circulation of bulk emails Controllers should: – use alternative methods of sending bulk emails opposed to CC/BCC when sending personal sensitive information – train staff on the risks and consequences of sending bulk emails in a non-compliant way – review and test current policies and updated guidance regularly to determine compliance and ensure that the policy considers the latest technologies/measures. This includes the notification, response, and reporting requirements in the event of a breach Recommendations from the ICO include: – delay emails being sent, allow the sender to review and if necessary, correct any errors before the email is sent – prompt alerts for users using CC / BCC fields – remove the auto-complete email function, preventing predictive input of email addresses – use the National Cyber Security Centre tool for analysing the security of an email.		

Development	Summary	Date	Links
Digital Regulation Cooperation Forum publishes technical study on age assurance technologies	Against the backdrop of the new Online Safety Act completing its passage through Parliament, the Digital Regulation Cooperation Forum published a technical study on the Measurement of Age Assurance Technologies. The study was commissioned by Ofcom and the ICO and seeks to improve their understanding of this area. It follows the commitment made by the regulatory bodies in November last year to maximise coherence between the data protection and online safety regimes and work. The study is *Part 2 – Current and short-term capability of a range of Age Assurance measures.* Part one of the study was a research report commissioned by the ICO (published last year) which explored four key pillars of the measurement of accuracy of age assurance technologies: *efficacy* (how well does it work?); *equality* (does it treat different people fairly and equally?) *comparability* (can you compare one type of age assurance component with the efficacy of another type of component?); and *repeatability* (can you repeat and reproduce the results of testing?). The Part 1 report concluded by setting out eight recommendations for the ICO to consider. Both reports are highly technical. The new Part 2 study provides information on the measurement of accuracy levels achievable by different age assurance solutions, and prompts further investigations on how to measure their overall effectiveness. The ICO and Ofcom note that they will continue to work together to ensure regulatory alignment in this area.	22 August 2023	Study (Part two) Study (Part one)
Connected tech: smart or sinister? **Second report on AI and creative technology**	The UK Culture Media and Sport Committee published its second report which focuses on AI and creative technology. The Government has two months to respond to these reports and the second report's findings include: – "while emerging technology can offer many benefits to the creative industries and their consumers, there are also a range of risks and harms associated with their use" – support for forthcoming AI regulation and a call for relevant regulators to be sufficiently trained in order to meet the demands placed on them. A discrete "AI regulation co-ordination unit" should be established to oversee progress	30 August 2023	Report

Development	Summary	Date	Links
	– emphasis that the approach to abandoning the text and data mining exemption to copyright is the correct one for the creative industry and work to rebuild the trust of the creative industries with appropriate licensing support is required – an evaluation on the applications of creative connected technology – from AR/VR to digital and AI generated art and encouragement for investment in "*a rich and diverse cultural and creative technology ecosystem*" – a recommendation that the Government address the issue of skills shortages in the forthcoming Cultural Education Plan – ensure creatives' rights are protected from AI generated media in the future – "*at minimum, this should involve bringing forward ratification of the Beijing Treaty on Audiovisual Performances by the time it responds to this report*". *By way of reminder, the Beijing Treaty is an international agreement to provide intellectual property rights in audiovisual performances. This was supported by the UK and signed in 2013 but has not been implemented / ratified. Whilst UK law meets most standard in the Treaty, some changes are required* It will be interesting to see how the Government responds to the Committee's recommendations in both AI and IP regulation, policy or guidance.		
12 challenges of AI governance	The UK Parliament's Science, Innovation and Technology Committee set out its interim findings in its inquiry into the impact of AI on different areas of society and the economy; whether and how AI and its different uses should be regulated; and the UK Government's AI governance proposals. The aim of the interim report is to highlight recent AI developments, the benefits and the challenges for policy makers. It reviews the Government's approach to date in comparison to that of other countries and "urges the Government to accelerate, not to pause, the establishment of a governance regime for AI, including whatever statutory measures as may be needed". The Government has 2 months to respond to the following recommendations/conclusions:	31 August 2023	Report

Development	Summary	Date	Links
	– awareness and use of AI continues to grow but it should not be seen as "magic" – it is "akin to other technologies: humans instruct a model or tool and use the outputs to inform, assist or augment a range of activities" – benefits of AI include transforming healthcare provision, improving the speed of data analytics, time saving, changing how education is delivered and assessed. "*Education policy must prioritise equipping children with the skills to succeed in a world where AI is ubiquitous*" – to ensure Government keeps up with the need to regulate, a gap analysis of the UK regulators is required to ensure they have the capacity, resource and powers to implement their new responsibilities – the new session of Parliament (post King's speech in November) will be the last opportunity before the General Election for the UK to legislate on the governance of AI – there is a risk of being left behind by other legislation (such as the EU AI Act) – the approach to governance and regulation should address the following 12 challenges and these should be a focus of the upcoming global summit in November: – the Bias challenge – AI can "introduce or perpetuate biases that society finds unacceptable" – the Privacy challenge – maintaining the protection of personal information – the Misrepresentation challenge - the generation of material that deliberately misrepresents someone's behaviour, opinions or character – the Access to Data challenge – AI needs large datasets to function well – the Access to Compute challenge – AI needs significant compute power which few organisations have – the Black Box challenge – transparency, not all AI can explain why they produce particular results – the Open Source challenge – open source promotes transparency and innovation vs proprietary code which		

Development	Summary	Date	Links
	will concentrate market power but may be more dependable – the IP and copyright challenge – using others content and protection of IP rights – the Liability challenge – if AI is used for harm then policy is required to establish if developers / providers bear liability for harms done – the Employment challenge – policy makers to anticipate and manage the disruption caused by AI in the employment market – the International Co-ordination challenge – AI is a global technology and so regulation should be an "*international undertaking*" – the Existential Challenge – if AI is a threat to human life the national security protections are required		
ICO Guidance: Information about workers' health	The ICO published guidance for employers to help them fully understand their data protection obligations under the UK GDPR and the DPA 2018 when handling workers' health data. The first part of the guidance explains how existing data protection law applies to the processing of workers' health data. The guidance reminds controllers that health data is a type of special category data which means that processing of the data is permitted only under limited circumstances with both a lawful basis and a special category condition. The guidance explains that there must be justifiable reasons for collecting data, it must be kept for only as long as is necessary and the reasons must be clearly communicated to the worker. It goes on to cover the lawful bases that are most likely to apply and the applicable special category conditions, including: Lawful bases – Where the processing is necessary for a contract with the worker, for example processing occupational sick pay – Complying with legal obligations (this does not cover contractual obligations), for example complying with health and safety obligations	31 August 2023	Guidance

Development	Summary	Date	Links
	– Legitimate interests of the employer or third party, for example to assist with a legal claim brought by the worker Special category conditions – Employment, social security and social protection law, for example maintaining maternity records – Legal claims or judicial acts, for example to assist with a legal claim brought by the worker – Substantial public interest, for example safeguarding children The guidance also sets out that a data protection impact assessment will usually be necessary given the sensitive nature of the workers' health information, and reminds controllers that all health information must be correct and that appropriate security measures are required, such as separate databases and access controls. The second part of the guidance looks at common employment practices and describes the legal requirements and good practice. This includes: – How to handle sickness and injury records – Occupational health schemes – Medical examinations and drugs and alcohol testing – Genetic testing – Health monitoring – Sharing workers' health information		
AI Safety Summit ambitions	The Government has set five objectives for the global summit in November to be held at Bletchley Park. These cover: – "a shared understanding of the risks posed by frontier AI and the need for action – *a forward process for international collaboration on frontier AI safety, including how best to support national and international frameworks*	4 September 2023	Statement

Development	Summary	Date	Links
	– *appropriate measures which individual organisations should take to increase frontier AI safety* – *areas for potential collaboration on AI safety research, including evaluating model capabilities and the development of new standards to support governance* – *how ensuring the safe development of AI will enable AI to be used for good globally"* The Government wants the summit to bring together global partners from government, tech and academia so the benefits of AI can be enjoyed by all safely. The Government has also published an introduction to the AI Safety Summit, reiterating its scope and announcing a number of pre-summit workshops (with the Alan Turing Institute, the British Academy, techUK and the Royal Society). The outcomes of these workshops are intended to feed into summit planning. There will also be a number of public Q&A sessions.		
ICO announces review of period and fertility tracking apps amid data security concerns	The ICO launched a call for evidence, urging users of period and fertility tracking apps to come forward to share their experiences. In addition, it has contacted a number of organisations that offer such apps in an effort to find out how they are processing users' personal information. The move comes as the results of a poll showed that more than half of women have concerns over their data is used by such apps and how securely it is kept. According to the poll, a third of women have used apps to track periods or fertility. In addition, over half of people who use the apps believed they had noticed an increase in baby or fertility-related adverts since signing up. 17% of poll respondents described receiving these adverts as distressing. The ICO is looking to understand whether the use of such apps carries a risk of harm and a resulting negative impact. It lists complicated privacy policies which leave users confused as to what they have signed up to, the collection and storage of excessive volumes of data, and users receiving upsetting and unwanted targeted advertising, as examples of such harms.	7 September 2023	Call for evidence ICO blog post

Development	Summary	Date	Links
	The National Data Guardian, Dr Nicola Byrne, and women's health groups have offered to support the ICO work in this area, which will include focus groups, user testing and working with key stakeholders. The deadline for responding to the call for evidence was 5 October 2023.		
Government publishes draft amendments to UK GDPR and DPA 2018 definition of "fundamental rights and freedoms"	The Government published the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 – a new statutory instrument to amend references to "fundamental rights and freedoms" in the UK's data protection legislation. In the accompanying explanatory memorandum, the Government explains that the current definition of "fundamental rights and freedoms" refers to rights retained under section 4 of European Union (Withdrawal) Act 2018 which will be repealed at the end of 2023. Before the UK's exit from the EU, "fundamental rights and freedoms" referred to those recognised in EU law and reaffirmed in the Charter of Fundamental Rights of the European Union. This included, the right to respect for private and family life, the right to freedom of expression and the right to protection of personal data. The new regulations will amend the meaning of "fundamental rights and freedoms" so that references to retained EU rights and freedoms are replaced with references to rights under the European Convention on Human Rights ("**ECHR**"), which has been enshrined in the UK's domestic law under the Human Rights Act 1998. The memorandum notes that the right most relevant in this context is the right to private life (Article 8 ECHR) and that other relevant rights including the right to freedom of expression will continue to be captured by the new definition. UK data protection legislation contains several references to "fundamental rights and freedoms", which come into play when – for example - the Government needs to consider making new conditions allowing the processing of special category data; or where it is restricting data subject rights on public interest grounds under Article 23(2) of the UK GDPR, and when controllers rely on the 'legitimate interests' lawful ground for processing.	11 September 2023	Statutory guidance Explanatory memorandum

Development	Summary	Date	Links
	The Government expects the impact on organisations and individuals as a result of these changes to be minimal because they seek to replicate the current position as far as possible, and it has no plans to publish guidance on the change. However, as the explanatory memorandum points out, there is no comprehensive or authoritative list of "fundamental rights and freedoms" which continue to be recognised in domestic law because of section 4 of EUWA 2018. Therefore, it is difficult to predict to what extent there will be an or any impact from this change. The new regulations will come into force immediately before the end of 2023.		
ICO announce 10 step guide to safeguard children when sharing personal information	The ICO published a ten step guide surrounding key data protection factors that must be considered when sharing personal information regarding child safeguarding purposes. The primary aim of this is to address concerns from both frontline workers and organisations who are unsure when they are able to share information without violating the UK General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR) and Data Protection Act 2018 – the "Data Protection Legislation". Recent case reviews involving children who have suffered serious harm or death due to abuse or neglect have highlighted the need for improving data sharing practices between organisations involved in the frontline care of children (for example schools, colleges, nurseries, healthcare settings, social work and social care providers). Insufficient information-sharing among the organisations involved in the children's care was a key contributing factor to slow response or failure to intervene in abuse and neglect. This guidance aims to provide practical advice in relation to data protection within the wider safeguarding context across ten points. The guidance reiterates the existing law and reminds organisations that they should understand that the Data Protection Legislation enables organisations to share data about vulnerable children and adults and that data can always be shared in emergency situations to prevent harm.	14 September 2023	Guide

Development	Summary	Date	Links
	The ICO reminds organisations that they should put in place strong systems and policies and review these regularly, building a culture of compliance and good practice. Organisations need to understand when safeguarding exemptions apply to individual rights requests. When sharing data regularly with other partners, they should put data sharing agreements (utilising the ICO's own data sharing code of practice) in place and regularly review and update DPIAs. The ICO reminds that when sharing information on a one-time basis, information can be provided if it is necessary and proportionate in the circumstances for the purposes of safeguarding the child.		
Government consults on potential benefits and implications of establishing Smart Data scheme	DSIT launched a consultation on the on the potential benefits and implications of establishing a Smart Data scheme – "Open Communications" in the UK's telecommunications market. The consultation explores whether there could be benefit in establishing a Smart Data scheme – "Open Communications" - in the UK telecoms market to help consumers make more informed choices about the services they buy. It follows the Government's Smart Data Review and continued work in this area, including the research into identifying ethical and trustworthy features of smart data, the future of smart data and a smart data implementation guide, by the Centre for Data Ethics and Innovation and the Department for Business, Energy and Industrial Strategy (released in July). The Government is seeking views from individuals, groups or organisations representing the individuals, groups, or organisations working in or representing: consumers of connectivity services; businesses or other public institutions that procure telecoms services; internet service providers (ISPs); mobile network operators (MNOs); mobile virtual network operators (MVNOs); and technology companies who may seek to use Open Communications data or are already within scope of a Smart Data scheme - such as price comparison websites and banks. The closing date for responses was 13 November 2023.	18 September 2023	Consultation Smart data review page Smart data research (July 2023)

Development	Summary	Date	Links
ICO and NCSC sign memorandum of understanding establishing framework for cooperation and information sharing	The Information Commissioner's Office ("**ICO**") and the National Cyber Security Centre ("**NCSC**") have published a memorandum of understanding establishing a framework for cooperation and information sharing. Their aim is to create a "*platform and mechanism to improve cyber security standards across the board while respecting each other's remits*". The MoU is a statement of intent and is not legally binding, it was signed by the Information Commissioner John Edwards and the NCSC's CEO Lindy Cameron. The MoU sets out how the NCSC and ICO will work together in a number of areas such as the development of cyber security standards and guidance by each party; information sharing; and deconfliction between the NCSC and the Commissioner in relation to incident management. In an accompanying news release, the ICO set out some of the key provisions of the MoU which include that the ICO will: – encourage organisations to engage appropriately with the NCSC on cyber security matters, including the response to cyber incidents – incentivise engagement with the NCSC, including by exploring how it can transparently demonstrate that meaningful engagement with the NCSC will reduce regulatory penalties – share information with NCSC about cyber incidents, on an anonymised and aggregate basis, as well as incident specific details where the matter is of national significance where the ICO and NCSC are both involved in a cyber incident, endeavour to deconflict to minimise disruption to an organisation's efforts to contain and mitigate harm – including by seeking to enable organisations to prioritise engagement with the NCSC and their partners in the immediate aftermath where that will prioritise mitigative work	12 September 2023	Memorandum of understanding

Development	Summary	Date	Links
UK-US data bridge approved for use from 12 October 2023	A new UK-US data bridge became available to businesses in the UK looking to transfer personal data to organisations in the United States certified under the UK Extension to the EU-US Data Privacy Framework ("**DPF**") from 12 October 2023, without the need for an additional transfer safeguard such as the UK's International Data Transfer Agreement or Addendum to the EU Standard Contractual Clauses. This is positive news for UK organisations. It expands the options available for transfers of personal data from the UK to the US. Organisations sending personal data to importers participating in the UK Extension to the EU-US DPF will not need to carry out a transfer risk assessment. The development also brings the UK's data transfer rules back in step with the EU. However, organisations should note that in their review of the UK-US data bridge, the UK's Information Commissioner identified areas that "*could pose some risks*" to UK data subjects if the protections identified (including clearly specifying any transfers of certain categories of sensitive personal data) are not properly applied. Read our full briefing for our full analysis of the UK-US data bridge.	21 September 2023	Press release
UK CMA report on and principles for development and use of AI foundation models	In May, the Competition and Markets Authority ("**CMA**") carried out an initial review of competition and consumer protection considerations in the development and use of AI foundation models ("**FMs**"). These are large, machine learning models trained on vast amounts of data that can be adapted to a wide range of tasks. Examples of FM uses include generative AI and chatbots. The CMA was tasked with considering the potential evolution of competitive markets for FMs; risks and benefits for competition and consumer protection; and development of guiding principles to support competition and protect consumers. The CMA then published a report on its findings from the review, together with proposed principles which "*aim to ensure consumer protection and healthy competition are at the heart of responsible development and use of FMs*".	18 September 2023	Report

Development	Summary	Date	Links
	This is essential reading for all organisations that currently develop, use or deploy AI foundation models, or may wish to do so in the future. Key findings of the report include: – developing a FM requires access to computing power, data, technical expertise and capital – good outcomes that could be generated by FMs include new and better products and services, easier access to information, assistance with both creative and administrative tasks and scientific and health breakthroughs – FMs have a potentially pro-competitive impact, facilitating the entry of more players into impacted markets, with consequent positive impact on pricing and productivity – conversely, if competition is weak, for example due to the prevalence of closed source FMs or the absence of freely available training data, this could cause harm, in the short term due to the spread of false information, AI-enabled fraud and fake reviews, and in the longer term due to market power resting with a few players – other factors, outside the scope of the CMA's remit, are also relevant to positive market outcomes, including safety, security, privacy, intellectual property rights and human rights The proposed principles are: – access – to data, computing power, technical expertise and funding – diversity – of business models, both open and closed source – choice – of deployment options – flexibility – interoperability of FMs and easy switching for consumers – fair dealing – no anti-competitive conduct – transparency – to help informed choices		

Development	Summary	Date	Links
	The CMA will now undertake a programme of engagement with UK and international stakeholders to further develop the principles. It plans to publish an update on the principles in early 2024.		
Inquiry launched into cyber resilience of UK's critical national infrastructure	The UK Science, Innovation and Technology Committee launched an inquiry into the cyber resilience of the UK's critical national infrastructure ("**CNI**"). The Committee reports that the UK is the third most targeted country in the world for cyber-attacks, with only the US and Ukraine experiencing a greater number. It states that "*Digital infrastructure is critical for supporting growth and helping to transform the delivery of public services….Much of the UK's CNI is underpinned by this digital infrastructure, which must be resilient to cyber-attack if it is to fulfil such fundamental roles in the UK economy*". The inquiry will consider progress towards 2025 cyber resilience targets, support needed to achieve targets and to make hardware architecture more secure by design, as well as the best approach by Government towards standards and regulations in this area. As part of the inquiry the Committee has launched a call for evidence. Submissions can be made until 10 November 2023, and are invited on the topics of: – types and sources of cyber threat to that CNI which is most critical to the function of the UK's digital economy, which it identifies as communications, energy, government and finance – views on the National Cyber Strategy 2022 and the Government Cyber Security Strategy 2022 – 2030 – effectiveness of strategic leads in this area and Government relationships with private sector operators and regulators – interventions required to ensure achievement of 2025 cyber resilience targets – the role of "secure by design" and emerging tech	September 2023	Inquiry Call for evidence

Development	Summary	Date	Links
	All organisations involved in the CNI digital infrastructure supply chain should consider responding with their views to help shape policy and future regulation in this area.		
Online Safety Bill in final form	(**NOTE**: On 26 October 2023, the Bill received Royal Assent to become the Online Safety Act, shortly before publication of this edition. We will keep you informed of developments.) The Online Safety Bill completed its journey through Parliament and is expected to receive Royal Assent and become law in the next few weeks. However, secondary legislation and guidance by Ofcom, the Bill's regulator, will be required before the Bill can fully come into force. The Bill will impose duties of care on providers of services that host user-generated content and search engines. The duties of care include requirements to: – undertake illegal content risk assessments – remove illegal content – use age verification to ensure that users of sites publishing or hosting pornography are at least 18 years old – undertake separate risk assessments in respect of services accessed by children and to protect children's online safety – operate systems and processes that allow affected persons to report illegal content Providers of user-to-user services that are categorised as Category 1 services (on the basis of user numbers and functionalities) will also be subject to enhanced duties. These include: – taking down material that breaches their own terms of service (so if those terms ban certain types of legal but harmful content, they will be required to take that type of content down) – offering adult users the option of verifying their identity – giving adult users the ability to block people who have not verified their identity	19 September 2023	Press release

Development	Summary	Date	Links
	– providing tools for adult users to choose whether or not they see legal but harmful content – protecting content of democratic importance and journalistic content.		
AI and Digital Hub to be launched by DRCF	The Department for Science, Innovation and Technology has announced a pilot scheme that will come into operation next year. This multi-agency service, run by members of the Digital Regulation Cooperation Forum, will support businesses in ensuring that their AI and digital innovations are compliant with regulatory standards. The press release says that "*This pilot scheme will meet business demands for coordinated support and help innovators navigate regulations, so they can spend more time developing cutting edge new products*".	19 September 2023	Press release

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

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

Tanvi Shah
Associate

Rebekah Whittington
Associate

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

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

Pooja Kohli
Associate

Soroosh Faegh
Associate

Rachel May
Associate

Development	Summary	Date	Links
New York Department of Financial Services Updates Cybersecurity Requirements for Financial Services Companies	The New York Department of Financial Services ("**NYDFS**") has revised its Part 500 Cybersecurity Requirements for Financial Services Companies with aim of strengthening cybersecurity practices and protocols for entities under its jurisdiction. Initially issued on July 29, 2022, these revisions were introduced by NYDFS on June 28, 2023, and the period for public feedback concluded on August 14, 2023. If these modifications receive the green light, covered entities will be granted a 180-day period from the effective date to align themselves with the updated requirements, with specific sections subject to varying compliance schedules.	28 June 2023	Regulations - Financial Services: Revised Proposed 2nd Amendment to Regulation 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies

Colorado Privacy Act Goes Into Effect	The Colorado Privacy Act ("**CPA**") is comprehensive legislation extending consumer rights and protections, as well as imposing compliance obligations on businesses in connection with data privacy. Entities, including non-profit organizations, that engage in business activities affecting more than 100,000 consumers annually within Colorado or derive profit from the sale of personal information from 25,000 or more Colorado residents may face civil penalties of up to $20,000 per violation for failure to comply with the new sets of rules outlined in the CPA, provided that any such violation is not rectified within a period of sixty (60) days. Some of the more significant provisions within the CPA are detailed as follows: (1) requiring consent for processing activity; (2) requirements for valid consent; (3) limited personal data processing under prior consent; (4) re-seeking and refreshing consent; (5) data minimization; (6) profiling; (7) universal opt-out mechanisms; (8) consumer loyalty programs; (9) data protection assessments; (10) exercising of consumer rights; (11) rights access; and (12) notice of changes to privacy policy. Colorado Attorney General Weiser announced the launch of enforcement of the CPA on July 12, 2023. As part of the enforcement effort, the Department began mailing letters to businesses focused on educating them about the new legal obligations pursuant to the CPA. The CPA went into effect on July 1, 2023.	1 July 2023	Colorado Privacy Act (CPA) - Colorado Attorney General | Colorado Attorney General (coag.gov)
Connecticut Personal Data Privacy and Online Monitoring Act Goes Into Effect	The Connecticut Personal Data Privacy and Online Monitoring Act ("**CTDPA**") is a new law that protects the online privacy of Connecticut residents and gives them more control over who uses their data. Under the CTDPA, Connecticut consumers have the right to: (1) know whether their data is being processed; (2) opt out of having their data used for certain purposes, such as targeted advertising; (3) get copies of their data in a portable format; and (4) request corrections to their data. The CTDPA applies to businesses and organizations that process the personal data of Connecticut residents. A "processor" is someone or a company that processes personal data on behalf of someone else. A "controller" is someone or a company that decides how and why personal data is processed. The CTDPA applies to any business or organization that: (1) does business in Connecticut or targets its services or products to Connecticut residents; (2) processed or controlled the personal data of 100,000 or more consumers in the past year; (3) processed or controlled the	1 July 2023	AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

	personal data of 25,000 or more consumers in the past year and earns more than 25% of its revenue from selling personal data. Some entities are exempt from the CTDPA, such as colleges and universities, non-profits, government contractors that process data for the government, and entities subject to the Gramm-Leach-Bliley Act of 1999 or the Health Insurance Portability and Accountability Act of 1996. The CTDPA went into effect on July 1, 2023.		
Eleventh Circuit: Individualized Issues May Predominate Standing Inquiry in Data-Breach Class Action	In the spring of 2018, Chili's was hit with a cyberattack in which customers' credit and debit card information was accessed and published on the dark web. Information for approximately 4.5 million payment cards was posted on a site called Joker Stash, which is an online market place for stolen payment data. Separate putative class actions (later consolidated) were brought against Chili's owner, Brinker International, by three different plaintiffs. The consolidated complaint asked for injunctive relief and damages and sought certification under Rule 23(b)(3) of two damages classes: a nationwide class, with claims for negligence; and a California class for violation of the California consumer-protection statute. The proposed class definition included all consumers who made a credit or debit card purchase at any affected Chili's location during the period of the data breach. The district court certified both classes but narrowed the class definition. Under the district court's order, the classes both were limited to consumers who both had their data accessed and incurred reasonable expenses or spent time spent mitigating the consequences of the data breach. The Eleventh Circuit granted Brinker's application for immediate appeal under Rule 23(f). Brinker raised three issues on appeal: plaintiffs lacked Article III standing; their claims will require individual mini-trials; and plaintiffs presented no reliable methodology for determining damages on a class-wide basis. The court vacated the decision in part, cutting out the claims of two of the three named plaintiffs for lack of standing and remanding to the district court for further analysis of Rule 23(b)'s predominance requirement, specifically as to the standing of absent class members.	11 July 2023	Individualized Issues May Predominate Standing Inquiry in Data-Breach Class Action - Eleventh Circuit Business Blog (11thcircuitbusinessblog.com)
California Announced Investigative Sweep; Sends Inquiry Letters to Large CA Employers Requesting	California's Attorney General ("**AG**") launched an initiative to investigate employers who are not following the California Consumer Privacy Act and California Privacy Rights Act (collectively, the "**CCPA**"). In early 2023, the CCPA's disclosure	14 July 2023	California Consumer Privacy Act Investigative Sweep (natlawreview.com)

Company Compliance Information Regarding CCPA	requirements and consumer rights provisions began to apply to job applicants, employees (and their beneficiaries), and independent contractors. Now, the AG's office has started sending out letters to California employers asking about their CCPA compliance. This is a major step forward in enforcing the CCPA, and this initiative focuses on employee data. The first set of letters went to large California employers, but it serves as an indication of broader enforcement action to come.		
Oregon Passes Comprehensive Privacy Law (Senate Bill 619)	On July 18, 2023, Oregon Governor Tina Kotek signed a new law called the Oregon Consumer Privacy Act ("**OCPA**"). The OCPA takes effect on July 1, 2024. It is similar to privacy laws passed in other states, such as Colorado, Virginia, Utah, and Connecticut. The OCPA applies to most businesses that operate in Oregon and collect or process the personal data of at least 100,000 Oregon residents, or at least 25,000 Oregon residents and make at least 25% of their revenue from selling personal data. There are a few exceptions to the OCPA. It does not apply to employment or business-to-business data. It also does not apply to protected health information processed in accordance with HIPAA, or to data that is collected or processed in accordance with certain federal laws, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Driver's Privacy Protection Act, and Family Educational Rights and Privacy Act. The OCPA also contains a broad exemption for personal health information, which includes: (1) information processed by HIPAA-covered entities; (2) data that is intermingled with and indistinguishable with HIPAA-covered information; and (3) several other health and medical research related data uses. Additionally, the OCPA does not apply to insurers, publishers, radios, and television stations. The OCPA also excludes de-identified data and publicly available data from its definition of "personal data."	18 July 2023	Microsoft Word - Document1 (oregonlegislature.gov)
FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies	The Federal Trade Commission ("**FTC**") and the U.S. Department of Health and Human Services' Office for Civil Rights ("**OCR**") are warning hospitals and telehealth providers about the privacy and security risks of using online tracking technologies on their websites and mobile apps. These technologies can collect sensitive personal health data about users without their knowledge or consent, and disclose it to third parties, such as advertisers. The FTC and OCR sent a letter to approximately 130 hospital systems and telehealth providers to alert them about the	20 July 2023	FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies | Federal Trade Commission

	risks of using tracking technologies, such as the Meta/Facebook pixel and Google Analytics. These technologies can gather identifiable information about users, such as their health conditions, diagnoses, medications, medical treatments, and frequency of visits to health care professionals. The disclosure of such information to third parties can have serious consequences, such as revealing sensitive information about a person's health and where they seek medical treatment. The FTC and OCR reminded entities covered by the Health Insurance Portability and Accountability Act (HIPAA) of their responsibilities to protect health data from unauthorized disclosure under the law. Companies not covered by HIPAA also have a responsibility to protect against the unauthorized disclosure of personal health information. The FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule.		
SEC Adopts New Rules Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies	On July 26, 2023, the US Securities and Exchange Commission SEC released final rules requiring disclosure by public companies of material cybersecurity incidents and policies and procedures related to cybersecurity risk management, strategy, and governance ("**Cybersecurity Rules**"). The Cybersecurity Rules create new disclosure obligations for public companies subject to the reporting requirements of the Securities Exchange Act of 1934, as amended, including business development companies and foreign private issuers. New disclosure obligations include: disclosure of cybersecurity incidents that detail the nature, scope, timing, and impact of such incidents; and disclosure of a registrant's risk management, strategy, and governance regarding cybersecurity risks, including the board of directors' oversight of cybersecurity risks and the impact of any such risks on its business strategy, results of operations and financial condition. Regardless of industry, the Cybersecurity Rules will require registrants to evaluate their current cybersecurity risk management practices. Given the short compliance timeline, registrants should begin evaluating whether their current cybersecurity policies and procedures, if any, account for the disclosure items contemplated by the Cybersecurity Rules.	26 July 2023	SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies SEC adopts new rules to expand public company disclosure relating to cybersecurity by year end - Eversheds Sutherland (eversheds-sutherland.com)

Oregon Passes Law Requiring Data Broker Registration	Oregon is the third state to require data brokers to register before collecting, selling, or licensing personal information. The law takes effect on January 1, 2024. Several types of businesses are exempt from the law, including companies that collect information from their customers or subscribers, consumer reporting agencies, financial institutions, and affiliates or non-affiliated third parties of financial institutions subject to the Gramm-Leach-Bliley Act. Companies that are subject to the law must register with the Department of Consumer and Business Services. The registration process includes paying a fee and providing a declaration that describes whether consumers can opt-out of all or a portion of the data activities, how the consumer can exercise their opt-out choices, and whether an authorized agent can do so on the consumer's behalf. Companies that fail to register as required face penalties of up to $500 per day, with a maximum penalty of $10,000 per calendar year. The law does not define what constitutes a "sale" of brokered personal data. However, the term "license" is defined as granting access to or distributing brokered data to another person for consideration. If you are a business that collects and sells or licenses personal information about people, consider reviewing the Oregon data broker registration law to determine if it applies to you. If you are subject to the law, you would need to register with the DCBS by January 1, 2024.	27 July 2023	Oregon's new data broker registration law - Lexology
CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies	The California Privacy Protection Agency's ("**CPPA**") Enforcement Division announced that it would review data privacy practices promulgated by connected vehicle ("**CV**") manufacturers and related CV technologies given that these vehicles are equipped with numerous features that potentially implicate sensitive data of users (such as GPS and location sharing, smartphone integration, and cameras). These vehicles constantly collect and gather sensitive user data like location and specific personal preferences about its users on a daily basis, so certain data privacy considerations are implicated. CPPA's Executive Director, Ashkan Soltani, said "Modern vehicles are effectively connected computers on wheels. They're able to collect a wealth of information via built-in apps, sensors, and cameras, which can monitor people both inside and near the vehicle." Soltani further stated that the CPPA's Enforcement Division is making inquiries with relevant parties to better understand how certain companies are (or are not) in endeavoring to remain in compliance with	31 July 2023	CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies (ca.gov)

	California law when collecting and utilizing the data of its consumers.		
New York Unveils New Cybersecurity Strategy to Safeguard from Cyber Threats	On Aug. 9, Governor Kathy Hochul unveiled New York State's cybersecurity strategy to protect the state's digital infrastructure from modern cyber threats. The plan sets goals, clarifies who is responsible for what, and coordinates different initiatives. It is designed to help all organizations, public and private, reduce their cyber risk and protect their critical infrastructure, networks, data, and technology systems.	9 August 2023	2023-NewYork-CybersecurityStrategy.pdf (ny.gov)
FTC Orders Experian Consumer Services to Pay $650K Settlement for Violating CAN-SPAM Act	The Federal Trade Commission ("**FTC**") has ordered Experian Consumer Services to pay a $650,000 settlement for violating the CAN-SPAM Act by sending unsolicited marketing emails to consumers without providing a clear way to opt-out. The FTC alleged that Experian spammed consumers with marketing offers after they signed up for an account to manage their Experian credit reports. These emails did not clearly inform recipients that they could opt-out of future marketing messages, which is a violation of the CAN-SPAM Act. The settlement order, which is pending court approval, requires Experian to include an opt-out mechanism in all future marketing emails. Experian said in a statement that it disagrees with the FTC's allegations, but that it has agreed to the settlement in order to move forward and focus on serving consumers. The company said that it has already implemented the changes requested by the FTC and introduced new ways for consumers to manage their emails.	14 August 2023	FTC Charges Experian with Spamming Consumers Who Signed Up for Company Accounts with Marketing Emails They Couldn't Opt Out Of | Federal Trade Commission
National Institute of Standards and Technology Releases Draft of Government's Cybersecurity and Privacy Learning Program	On August 28, the National Institute of Standards and Technology released a draft document with recommendations for developing and managing a cybersecurity and privacy learning program ("**CPLP**"). The document emphasizes the importance of integrating privacy with cybersecurity, using a life-cycle model, and aligning the CPLP with organizational goals. The public comment period for the draft document is open until October 27, 2023.	28 August 2023	NIST SP 800-50r1 initial public draft, Building a Cybersecurity and Privacy Learning Program
California Privacy Protection Agency Releases Draft Regulations for Risk Assessments and Cybersecurity Audits	The CPPA is making new rules for businesses that collect and use personal information about California residents. These rules are designed to protect consumers' privacy and security. The new rules will require businesses to: (1) assess the risks associated with their processing of personal information; (2) implement	8 September 2023	DRAFT RISK ASSESSMENT REGULATIONS FOR CALIFORNIA PRIVACY PROTECTION AGENCY SEPTEMBER 8, 2023 BOARD

	processes to mitigate those risks; (3) have their cybersecurity practices audited by certified experts. The CPPA can take action against businesses that do not comply with these rules. The new rules are intended to help protect consumers' privacy and security.		MEETING DRAFT CYBERSECURITY AUDIT REGULATIONS FOR CALIFORNIA PRIVACY PROTECTION AGENCY SEPTEMBER 8, 2023 BOARD MEETING
CFPB Proposal Signals Dramatic Expansion of the Fair Credit Reporting Act to Data Brokers	On September 15, 2023, the Consumer Financial Protection Bureau ("**CFPB**") published an outline of expansive rulemaking proposals to modernize the coverage of the Fair Credit Reporting Act ("**FCRA**") to include data brokers, data aggregators, and alternative data sources. In its FCRA proposal, the CFPB focused on two objectives: (1) Data broker regulation; and (2) Removal of medical debt from consumer reports. The CFPB plans to achieve these objectives primarily by broadening its interpretation of two interconnected definitions that determine coverage under the FCRA and thus shape the legal landscape of digital marketing, data brokering, and aggregation: "consumer reports" and "consumer reporting agencies". Entities that rely upon data sourced by alternative data resources such as data brokers, data aggregators, lead generators, and online resources to assist entities capture information about visitors to their apps and website, and for online advertising, should take a close look at the modernized interpretations of "consumer report" and "consumer reporting agency" that the CFPB is proposing. This long-awaited FCRA Proposal, together with the CFPB's consumer financial data rulemaking under Section 1033, would expand entities' responsibilities for assuring they obtain consumer permission to collect, use and disclose consumers' information, especially when sharing, analyzing or aggregating that information using artificial intelligence. Moreover, entities that would ultimately meet the expanded view of "consumer reporting agencies" would need to be accountable to rigorously comply with FCRA's "permissible purpose" requirements before disseminating consumers' FCRA protected information.	15 September 2023	CFPB proposal signals a dramatic expansion of the Fair Credit Reporting Act to data brokers - Eversheds Sutherland (eversheds-sutherland.com)
New York Department of Financial Services Issues Proposed Updated Expectations on Adoption or Listing of Virtual Currencies	The New York State Department of Financial Services ("**DFS**") is making new rules for virtual currency businesses. These rules are designed to make the DFS a better regulator of virtual currency in the United States. The new rules would require virtual currency businesses to do things like: Carefully assess the risks of listing	18 September 2023	Press Release - September 18, 2023: DFS Superintendent Adrienne A. Harris Announces Update On Two Year Transformational Initiative to

	and delisting coins and tokens Have a plan for delisting coins and tokens that no longer meet DFS's standards Get DFS's approval before listing or delisting any coins or tokens The new rules also update the DFS Greenlist, which is a list of coins and tokens that DFS has approved for virtual currency businesses to list or custody. The DFS is looking for feedback on the new rules until October 20, 2023.	Strengthen DFS' Nation-Leading Virtual Currency Oversight | Department of Financial Services (ny.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

Follow Eversheds Sutherland's global **Data, Privacy and Cybersecurity team** on LinkedIn.

Editorial team

Lizzie Charlton
Data Privacy Professional Support Lawyer
T: +44 20 7919 0826
lizziecharlton@
eversheds-sutherland.com

Krishan Jadav
Trainee Solicitor
T: +44 20 7919 0968
krishanjadav@
eversheds-sutherland.com

Jade Driscoll
Trainee Solicitor
T: +44 1223 44 3659
jadedriscoll@
eversheds-sutherland.com

Agata Lawrenciow
Trainee Solicitor
T: +44 20 7919 4917
agatalawrenciow@
eversheds-sutherland.com

Anya Lowton
Trainee Solicitor
T: +44 113 200 4094
anyalowton@
eversheds-sutherland.com

Rumaysah Khan
Apprentice Solicitor
T: +44 20 7919 0921
rumaysahkhan@
eversheds-sutherland.com

Jessica Ouchai
Trainee Solicitor
T: +44 20 7919 4813
jessicaouchai@
eversheds-sutherland.com

Rana Younis
Trainee Solicitor
T: +44 121 232 1298
ranayounis@
eversheds-sutherland.com

eversheds-sutherland.com

Updata Edition 21