EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

January to March 2023

Executive summary

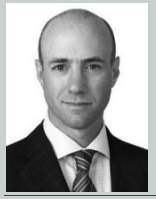
Welcome to the latest edition of Updata!

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 January to March 2022 and is full of newsworthy items from our team members around the globe, including:

- artificial intelligence (AI) is a heavy focus across the globe, with more updates on the **European Commission's new AI Act**, new **guidance from the ICO** on AI and data protection, a restriction of processing order by the **Italian DPA** due to the use of AI in chat-bots, and new US **NIST AI Framework Guidance on Risk Management and Governance for Trustworthy AI Systems**;
- international data transfers to the U.S continue to attract discussion in the EU and UK, with the **European Data Protection Board's Opinion** on the draft EU-US Data Privacy Framework adequacy decision and the **UK-US Joint Statement** on the progress towards adequacy;
- appropriate **consent to and disclosure of cookies** continues to be a primary focus of global regulators;
- the UK's **landmark data adequacy decision** with South Korea comes into effect;
- the introduction by the UK Government of the **Data Protection and Digital Information (No. 2) Bill,** replacing the previous Bill and with a purpose of updating and simplifying the UK data protection framework;
- a ruling from the **Austrian Court** that in certain circumstances, a privacy policy can form part of the consumer contract;
- the referral of the European Commission of **eight EU Member States** to the Court of Justice for failure to transpose and notify the national measures transposing the whistleblowing directive (Directive (EU) 2019/1937);
- issuance by the **Cyberspace Administration of China** of the Measures on the Standard Contract for the Outbound Transfer of Personal Information and a template standard contract;
- new guidance from the **Czech Republic's** Office for Personal Data Protection on cookies and consent, while the Munich I Regional Court in **Germany** rules that the cookie banner of a major German media platform is unlawful;
- the **Korea-Singapore Digital Partnership Agreement's** entry into force on 14 January 2023 as well as three **Memorandums of Understanding** implementing the Korea-Singapore Digital Economy Dialogue;
- new legislation in **Poland** regarding remote working for employees, including a requirement by employers to develop a procedure for the protection of personal data in remote work; and
- the **Virginia Consumer Data Protection Act** and **California Privacy Rights Act** take effect.

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



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

Follow us on Twitter at:

@ESPrivacyLaw

General EU and International

Contributors

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

Carolyn Sullivan
Associate
T: +44 20 7919 0941
carolynsullivan@
eversheds-sutherland.com

Development	Summary	Date	Links
EU AI Act	With organisations increasingly relying on AI technology, UK and EU regulators are turning their attention to effective regulation of AI in an effort to recognise its benefits while instilling confidence in individuals that the increasing use of AI is being deployed appropriately and lawfully. In the EU, the compromise text of the European Commission's AI Act was approved by the Council of the EU on 6 December 2022. The European Parliament is expecting to adopt the AI Act by the end of 2023. The AI Act is expected to lead the framework for the regulation of AI in and outside the EU. Much like the GDPR in terms of impact, the AI Act will have an extra-territorial scope, extending to providers and users outside the EU where the output is used in the EU. This is anticipated as being a benchmark AI law which other jurisdictions might look towards when developing their own laws (much like GDPR has become a standard upon which some other countries' own laws are heavily based). Organisations deploying AI systems may wish to consider the AI Act (in its current form) now, in particular the responsibilities of providers with respect to those systems, in order to develop their processes accordingly. In a similar vein to "privacy by design" as is required by GDPR, the AI Act (if passed into law) means AI system providers will need to bear these obligations in mind when developing AI systems.	January 2023	Eversheds Sutherland Article on EU AI Act Eversheds Sutherland Article: Commonalities between the EU and US for the AI march to regulatory change
Tech company fined for imposing cookies	A global tech company which operates an online search engine in the EEA has been fined €60 million for making it too hard for users to refuse optional cookies. After complaints from	January 2023	

Development	Summary	Date	Links
	individuals, the French data protection regulator, the CNIL, launched several investigations on the website in September 2020 and May 2021. When visiting the tech company's site, the CNIL found that a pop up window asked if users wanted to accept the cookies or if they wanted to explore more options. Refusal of the cookies required two clicks, by clicking "more options" and then "disable", whereas to "accept" was only one click. CNIL therefore outlined that the refusal of cookies was more burdensome, as it required more steps than accepting the cookies and it was unclear if "disable" meant refusal. Based on the tech company's financial capacity and the fact it indirectly generated profit from the optional cookies being placed, the CNIL justified a €60 million fine. Whilst the fine was levied in France, this serves as a useful reminder to website-owners (including in the United Kingdom) to ensure that it is as easy for individuals to opt-out of optional cookies as it is to accept them.		
Clarification provided on the scope of the right to receive personal data by the Austrian Advocate General – data subject access requests	The Austrian Advocate General has provided clarification on the right for data subjects to receive a copy of their personal data under Article 15 GDPR. The Advocate General's Opinion on this topic was requested on a number of questions referred by the Federal Administrative Court in Austria. Some of the key clarifications made by the Advocate General are as follows: 1. the meaning of a 'copy' – a copy comprises a faithful reproduction in an intelligible form of the personal data requested by the data subject. The copy must be in a material and permanent form. The exact form of the copy will vary on a case by case basis depending on the specific circumstances of the case and the needs of the data subject 2. should the full document be provided – the Advocate General stated that the right of access does not grant a general right of access for the data subject to obtain a full or partial copy of the document that contains their personal data. However, the controller should provide documents	January 2023	Advocate General Clarification

Development	Summary	Date	Links
	where it would be necessary to ensure that the personal data is intelligible 3. meaning of 'information' in the third sentence of Article 15(3) GDPR – the term 'information' should be interpreted as "the copy of personal data undergoing processing", as it is in the first sentence of 15(3) This Opinion, provided on 15 December 2022, is not binding on the CJEU, nor is it binding in the UK. However, it provides helpful clarification on GDPR Article 15 and for the most part, the CJEU follows the Advocate General's opinions in subsequent cases.		
CJEU clarifies whether controllers must provide the specific identity of recipients of personal data	The CJEU has issued a preliminary ruling regarding the disclosure of personal data by controllers. The Claimant asked the Austrian postal service to disclose the identity of recipients to whom it had disclosed their personal data, as part of the Claimant's right to access under GDPR. In response, the Austrian postal service stated that it used personal data to the extent permissible by law, in the course of its activities as a publisher of telephone directories. It later informed the Claimant that their data was also forwarded to advertisers, IT companies and mailing list providers. Therefore the Austrian postal service provided the categories of recipients, but not their specific identity. The Supreme Court in Austria referred the case to the CJEU for a preliminary ruling on whether the GDPR requires the controller to disclose the specific identity of the recipients. The CJEU ruled that where personal data has been or will be disclosed to recipients, there is an obligation on the part of the controller to provide the data subject, on request, with the actual identity of those recipients. However, the CJEU noted that: 1. in situations where it isn't currently possible to identify recipients (such as where they are not yet known), the controller may indicate only the categories of recipient in question; and	January 2023	CJEU Ruling

Development	Summary	Date	Links
	2. in situations where the controller can reasonably demonstrate that any request is excessive or unfounded, they may indicate only the categories of the recipient in question. This ruling is also noteworthy from a UK GDPR perspective. Although not binding in the UK, it does highlight what is required from an EU perspective for when individuals exercise their right of access. The ICO may also look to such rulings as being informative in determining what approach to take under UK GDPR.		
The European Commission decides to refer 8 Member States to the Court of Justice of the European Union over the protection of whistle-blowers	The European Commission has decided to refer **Czechia**, **Germany**, **Estonia**, **Spain**, **Italy**, **Luxembourg**, **Hungary** and **Poland** to the Court of Justice for failure to transpose and notify the national measures transposing the whistleblowing directive (Directive (EU) 2019/1937). The directive requires Member States to provide whistle-blowers working in the public and private sectors with effective channels to report breaches of EU rules confidentially, establishing a robust system of protection against retaliation. Member States had to transpose the necessary measures to comply with the Directive's provisions by 17 December 2021.	15 February 2023	Press Release
The Digital Euro in 2023	Cash is the most "privacy-friendly" means of payment in an increasingly digitalised world. Recently, the European Central Bank ("**ECB**") has been asked by the European Data Protection Board to include safeguards and features similar to those found in cash to the future digital euro. In 2021, an investigation phase was launched by the ECB for the development of the digital euro which sees this as a complement to cash rather than a replacement. Transaction confidentiality has been found to be the most important requirement of the future digital euro to have success in competing in an already crowded payments market. Last October, the EDPB issued a statement inviting the ECB to consider its approach on three focal points: 1. the possibility of using the digital euro my way of an offline electronic wallet, without internet connection	February 2023	ECB Press Release

Development	Summary	Date	Links
	2. by way of avoiding generalised transaction tracing, a privacy threshold will be granted for online and offline use (below this threshold, transaction data would not be traced by the Eurosystem or intermediaries) 3. a specific legal regime for the digital eprivacy, data protection and the combat against money laundering and terrorist financing It has been said that 2023 will be a significant year for the digital euro project. The aim is to have a legislative proposal from the European Commission by the summer, which leaves a mere 5-6 months to plan and design a digital euro that appreciates privacy from the beginning.		
EDPB Opinion on draft EU-US Data Privacy Framework adequacy decision	On 28 February the European Data Protection Board ("**EDPB**") published its opinion ("**Opinion**") on the European Commission draft adequacy decision regarding the EU-US Data Privacy Framework ("**DPF**") which, if adopted by the European Commission, will provide for safe transfers of personal data from the EU to US companies which have joined the DPF and have agreed to comply with the DPF principles. The DPF replaces the previous US Privacy Shield (which was invalidated by the CJEU in the *Schrems II* case) and contains new US data privacy principles. The Opinion recognises substantial improvements to the level of protection for EU data subject rights offered by the DPF in comparison to that under the Privacy Shield. However, it also identifies some concerns and urges the European Commission to take steps to address those concerns before the adequacy decision is finalised. Particular recommendations and concerns raised include: 1. that the European Commission amends the draft decision to provide greater clarification on the scope of the exemptions where the DPF does not apply (e.g. to comply with a court order or meet public interest) and the safeguards under US law for these exemptions the draft decision requires a more consistent use of terminology and definitions;	28 February 2023	Opinion

Development	Summary	Date	Links
	2. the EDPB's concern about the rights of data subjects to access data and object to processing, particularly when data is transferred onwards from the initial recipient; 3. the need for clarity in the application of the DPF's principles to processors; 4. the need for specific safeguards in the area of automated decision making; and 5. compliance and oversight, particularly in relation to redress mechanisms. The Opinion is not binding but is expected to be followed by the European Commission. The draft adequacy decision will then be sent to representatives of the EU Member States for their approval.		

Austria

Contributors

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

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

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

Development	Summary	Date	Links
Austrian DPA: Use of Tracking Pixel of US-based Social Media Provider on Website violates GDPR and "Schrems II"	Following a complaint by the Austrian Privacy NGO "NOYB", the Austrian DPA ruled against a provider of a news website. The website had used certain tools offered by a US-based social media provider, including a tool for easy login as well as a tracking pixel for statistical purposes. The collected data were processed by the social media provider in the USA. The Austrian DPA ruled that the data processed was personal data. As this data was transferred to the USA and as the social media provider could not prove that they had taken measures to provide an adequate level of protection to the data transferred, the DPA ruled that the website provider had violated the GDPR by using said tools. The complaint against the social media provider was rejected, however, as the DPA deems that only the data exporter (in this case the website provider), not the data importer, is responsible for making sure a data transfer complies with the GDPR. The decision is not yet legally binding, as it can be appealed.	6 March 2023	Link to report on NOYB website (in English) Link to translation of decision to English provided by NOYB Link to a copy of the original decision provided by NOYB (in German)
Austrian Supreme Court: Privacy Policies are subject to the same review as B2C Terms and	A consumer association filed a class action lawsuit against an insurance company. In this case, the consumer association claimed that the defendant's Privacy Policy violated consumer	Date of Decision: 6 March 2023	Link to decision (in German)

Development	Summary	Date	Links
Conditions if a customer has to actively accept them	law, as its wording was unclear and not transparent. They claimed that the Privacy Policy should be considered as part of the consumer contract, as when concluding the contract, customers had to confirm that they had taken notice of the Policy. The defendant argued that a Privacy Policy was subject to the GDPR, not to consumer law. The Austrian Supreme Court ruled in favor of the consumer association. It ruled that the fact that customers had to confirm that they had taken note of the Privacy Policy was enough to make it part of the consumer contract. Therefore, the Privacy Policy had to comply with the extremely strict rules on B2C Terms & Conditions, which it did not. The Supreme Court thus ruled against the defendant. Based on this ruling, companies should, where possible, consider removing any request to the customer to actively confirm (e.g. tick-boxes) that they have taken note of the Privacy Policy from their contracts in Austria.	Published: 4 January 2023	Eversheds Sutherland newsletter entry on this decision (in German)
Austrian Constitutional Court repeals Media Privilege in Austrian Data Protection Act as unconstitutional	In this case, Eversheds Sutherland Austria represented the complainant in a proceeding at the Austrian DPA against a media provider, which led to a landmark ruling by the Austrian Constitutional Court. The Austrian Data Protection Act includes a privilege for data processing by certain media providers for journalistic purposes. Following an appeal against this privilege, the Austrian Constitutional Court ruled that this Media Privilege violated the Austrian Constitution and the Fundamental Right to Data Protection. The Court ruled that the fundamental Right to Data Protection may only be restricted insofar as this was absolutely necessary for certain purposes in the public interest. A general privilege for all data processing by media companies therefore goes too far and is unconstitutional. The provision (Sec. 9 (1) of the Austrian Data Protection Act) was therefore repealed. The Austrian legislator has a deadline of 30 June 2024 to replace the provision with one which complies with the constitutional rules.	Date of decision: 6 March 2023 Published: 9 January 2023	Link to decision (in German) Eversheds Sutherland newsletter entry on this decision (in German)

Development	Summary	Date	Links
Federal Administrative Court: Right to Data Portability does not apply to physical documents	A data subject filed a GDPR complaint at the Austrian DPA, requesting from the defendant copies of certain documents. He based this request on, among other things, the right to data portability (Article 20 GDPR). Following an appeal, the Austrian Federal Administrative Court ruled that the right to data portability does not apply to physical documents and cannot be used as a legal basis to request copies of physical documents. Instead, this right only applies to data that is processed automatically by computer systems, particularly by online platforms.	Date of Decision: 6 March 2023 Published: 4 January 2023	Link to decision (in German)
Federal Administrative Court: Customer Data purchased in Asset Deal may be used for Direct Marketing	In this case, a company had purchased an insolvent company's assets, including its online shop and customer database. It used this database to send direct marketing messages to its customers. The recipients had not consented to this, but the company referred to the exception of Article 13 (2) of the EU ePrivacy-Directive (and its Austrian implementation in Sec. 107 TKG 2003/Sec. 174 TKG 2021), which allows for direct marketing on an opt-out basis in relation to marketing sent to existing customers. However, a recipient filed a complaint to the Austrian DPA. They claimed that the named exception should not apply, as the complainant had not been a customer of the defendant, but of the company whose customer database had been purchased. They claimed that a purchaser of customer data should not be entitled to use this exception. Following an appeal against the DPA's decision, the Federal Administrative Court denied the complaint. It ruled that the exception of Article 13 (2) ePrivacy-Directive should apply to the owner of the business in an economic sense. As the defendant had purchased the insolvent company's business via an asset deal (including the online shop), they could reasonably expect the complainant to still be interested in the online shop's products. Therefore, they could rely on the exception of Article 13 (2) ePrivacy-Directive. As all other requirements of Article 13 (2) ePrivacy-Directive and its national implementation were met, the processing was permissible.	Date of Decision: 6 March 2023 Published: 23 January 2023	Link to decision (in German)

Austria

Development	Summary	Date	Links
Austrian DPA creates official online form for easier filing of GDPR complaints	The Austrian DPA has created a new online tool, where data subjects can easily file complaints or request the Austrian DPA to investigate alleged violations of the GDPR. This is intended to facilitate the filing of complaints.	1 February 2023	Link to online form
Austrian DPA: GDPR applies to data processing via a smartphone app as long as the app can be downloaded and used in the EEA	This case concerned the applicability of the GDPR to a US-based service provider offering chatroom services. A complainant filed a complaint to the Austrian DPA, as the respondent had not answered their Data Subject Access Request (DSAR) under Article 15 GDPR. The respondent argued (amongst other things) that the GDPR was not applicable at the time, as the respondent had not marketed its app to the EU/EEA. The customer-base was mainly from the USA, and only following an unexpected hype had there been an unintended influx of European users. The DPA ruled that it was irrelevant whether the app provider marketed its services to the EEA. The fact that the app could be downloaded and used in the EEA via the app store without restrictions was sufficient to make the GDPR applicable under Article 3 (2a) GDPR. Therefore, as the DSAR had not been answered, the DPA ruled against the app provider.	Date of Decision: 1 February 2023 Published: 6 March 2023	Link to decision (in German)
Data Breach – notification of data subjects is required when health data are unlawfully published for several hours on Social Media	The DPA ruled against a hospital operator, following a data breach notification. A trainee of the hospital provider had uploaded a photo to their "story" on a social media platform, making it accessible to approximately 100 people for several hours before it was deleted. In this photo, patient data was visible. The hospital filed a data breach notification to the Austrian DPA, but did not inform the affected data subjects as they did not assume any significant risk for these data subjects. The DPA ruled against the hospital and ordered them to inform the affected data subjects. The DPA argued that a data breach concerning health data usually poses a high risk for affected data subjects. Even if the data were accessible only to a limited	Date of Decision: 1 February 2023 Published: 15 March 2023	Link to decision (in German)

Development	Summary	Date	Links
	number of people online for a short period of time, the risk to the affected data subjects was still high, as data shared online can easily be copied and shared with other recipients. Therefore, the hospital was required to inform the affected data subjects of the data breach under Article 34 GDPR.		
Cybercrime: Austrian Government presents plans to introduce higher penalties and to increase police's investigative possibilities	The Austrian Government has presented a new legal initiative to fight against cybercrime. The proposed amendment to the Austrian Criminal Code includes higher penalties for certain cybercrimes. These higher penalties shall also provide for more investigative possibilities for the police. In the future, undercover investigations by the criminal police, including the establishment of a special unit called Cyber-Cobra, will make mobile phone tracking and prosecution abroad possible. After the law enters into force, a European arrest warrant could be obtained for such crimes and criminals could be extradited to Austria. Furthermore, the Government has stressed that prevention and awareness are the best protection against cybercrime. The new proposal is currently published for public review until 19 April 2023.	8 March 2023	Link to press statement (in German) Link to draft legislation (in German)

Belgium

Contributors

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

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

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

Development	Summary	Date	Links
Belgian Constitutional Court ruled that interested third parties, who were not parties to the proceedings before the BDPA, should be able to appeal directly before the Market Court	A third party-company, which was not previously involved in a procedure before the Dispute Chamber of the Belgian Data Protection Authority ("**BDPA**"), opposed the BDPA's decision before the Market Court, the appeal body of the Dispute Chamber of the BDPA. The Market Court declared the appeal inadmissible due to lack of jurisdiction in relation to the third party. The third party filed a second appeal against the BDPA's decision, but this time before the Council of State. The Council of State submitted several preliminary questions to the Constitutional Court. In its judgement of 12 January 2023, the Constitutional Court ruled that interested parties who were not involved in the proceedings before the BDPA should be able to lodge an appeal directly to the Market Court (rather than to the Council of State). The Constitutional Court based its decision on Article 78(1) GDPR, which stipulates that "each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them". It concluded that denying a third party the right of appeal to the Market Court violated the principle of equality. The Belgian legislator must now amend Article 108(1) of the Law of 3 December 2017 on the establishment of the BDPA to allow third parties to lodge an appeal against the decisions of the BDPA. The Constitutional Court also provided for a transitional period stating that as of 12th January 2023, each third party has	12 January 2023	Ruling (Dutch) Ruling (French)

Development	Summary	Date	Links
	the right to lodge an appeal against a decision of the BDPA, but only within 30 days of: (i) becoming aware of the decision of the BDPA, or (ii) the publication of the Constitutional Courts' ruling in the Belgian Official Gazette.		
BDPA issued a reprimand to a local authority following a complaint over the use of geolocation	On 21 February 2023, the Dispute Chamber of the Belgian Data Protection Authority ("**BDPA**") issued a reprimand to a Belgian local authority following a complaint about the geolocation system (with GPS-tracking) installed in their employees' cars. It ruled that the GPS tracking was unlawful for the following reasons: 1. the local authority first carried out the processing of the employees' personal data without a legal basis. Afterwards, it relied wrongfully on legitimate interest as a legal basis because a public authority is not allowed to rely on legitimate interest in the performance of its duties (Article 6.1 (f) in fine GDPR). Instead, they should have relied upon public interest; 2. the transparency obligation was breached as no information was provided to the employees about the GPS tracking (Article 5.1 (a) GDPR); 3. the accountability principle was breached as no adequate technical and organisational measures were taken by the local authority (Article 5.2 and 24 GDPR); 4. the privacy policy was poorly comprehensible and incomplete (e.g., the retention periods, contact details of the data protection officer (**"DPO"**), purposes and legal bases of the processing were not mentioned) (Articles 13 and 14 GDPR); and 5. the record of processing activities lacked contact data of the DPO (Article 30 GDPR). It should be noted that the BDPA did not rule out that such GPS tracking can be lawful under strict conditions.	21 February 2023	Decision (Dutch)

Bulgaria

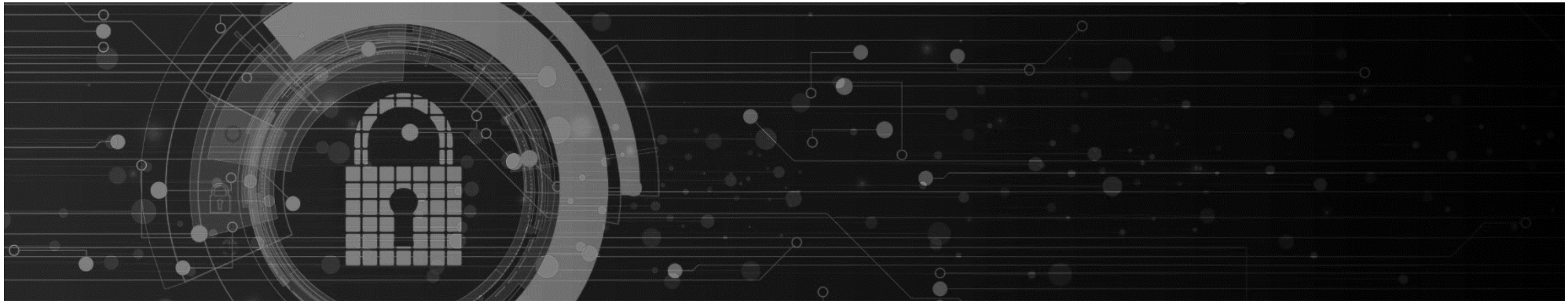
Contributors

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

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

Development	Summary	Date	Links
Judgement of the Court of Justice to the European Union regarding the collection of dactyloscopic and photographic data in the context of criminal investigations in Bulgaria	The Bulgarian authorities initiated criminal proceedings against two commercial companies for fraud concerning the setting and payment of tax obligations, where one of the accused persons refused to consent to the collection of the dactyloscopic (i.e. fingerprint) and photographic data concerning them. The accused person also refused to consent to the taking of a sample for the purpose of creating a DNA profile. The police did not collect the data and brought the matter before the referring court. The Specialised Criminal Court of Bulgaria decided to stay the proceedings and referred four questions to the Court of Justice to the European Union ("**CJEU**") for a preliminary ruling, which concerns the interpretation of Directive (EU) 2016/680 on 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 ("**Directive**") and Article 52 of the Charter of Fundamental Rights of the European Union ("**Charter**"). The CJEU ruled, among other things, that: 1. the fact that the legal basis for processing refers to the GDPR, and not to the Directive, is not capable, in itself, of calling the existence of such authorisation into question, despite the fact that the processing of biometric and genetic data at issue falls within the scope of the Directive, and not of the GDPR; and 2. Article 6(a) of Directive 2016/680 and Articles 47 and 48 of the Charter must be interpreted in a way that the criminal court, having jurisdiction, can authorise a measure enforcing the collection of the biometric and genetic data for record	26 January 2023	Decision

Development	Summary	Date	Links
	collection, without having the power to assess whether there are serious grounds for believing that the person concerned has committed the offence of which he or she is accused.		
The Commission for Personal Data Protection has new powers under the Bulgarian Whistleblowing Act	According to the Whistleblowing Act, the CPDP shall act as a central authority for external submission of reports. The CPDP shall also adopt new underlying legislation on the implementation of the Whistleblowing Act, including an ordinance on keeping a register of reports, as well as methodological instructions and model forms for registration of reports. The deadline for the adoption of such legislation is 4 August 2023.	10 February 2023	CPDP Powers
New guidelines of the Commission for Personal Data Protection regarding the implementation of the Whistleblowing Act	The Bulgarian Commission for Personal Data Protection ("**CPDP**") has published guidelines regarding the implementation of reporting channels under the newly adopted Whistleblowing Act 2023, as well as a roadmap which outlines the main stages of the implementation of the system for the protection of whistle-blowers. On 4 May 2023 a function for generating a Unique Identification Number ("**UNI**") will be put into operation on the website of the CPDP. This UNI must be used by the designated person in charge under Article 14 of the Whistleblowing Act. The external submission of signals to the CPDP is expected to become functional from 4 August 2023.	10 March 2023	Guidelines



China

Contributors

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

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

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

Development	Summary	Date	Links
Guiding Opinions of 16 Authorities on Promoting the Development of Data Security Industry 十六部门关于促进数据安全产业发展的指导意见	The Ministry of Industry and Information Technology and 15 other authorities have jointly released the Guiding Opinions on Promoting the Development of Data Security Industry ("**Opinions**"). The Opinions focus on data security protection and the demands for developing and utilizing relevant data resources, including: 1. proposing the overall requirements for promoting the development of the data security industry, which include the guiding thoughts and basic principles, and putting forward the industrial development goals by 2025 and 2035; 2. specifying seven key tasks for promoting the development of the data security industry from two perspectives, firstly, what actions should be taken by the industry itself, which includes four key tasks (i.e. raising industrial innovation capabilities, expanding data security services, promoting the building of standard systems and promoting the application of technical products), and secondly, how to support the industry, which includes three key tasks (i.e. building an ecology for industrial prosperity, strengthening the talent supply and deepening international cooperation and exchanges); and	3 January 2023	Guiding Opinions

Development	Summary	Date	Links
	3. stipulating the measures in three areas to implement the Opinions and effectively promote the healthy development of the industry, including strengthening organization and coordination, increasing policy support and optimizing the environment for industrial development.		
Practice Guidance on Cyber Security Standards — Verification of the Effects of Partial Contour Processing of Exterior Images of Vehicles (Draft for Comments) **网络安全标准实践指南—车外画面局部轮廓化处理效果验证（征求意见稿）**	On 6 January 2023, China's National Information Security Standardization Technical Committee ("**NISSTC**") issued the Practice Guidance on Cyber Security Standards — Verification of the Effects of Partial Contour Processing of Exterior Images of Vehicles (Draft for Comments) ("**Practice Guidance**"), which was open for public comment until 20 January 2023. The Practice Guidance is designed to guide vehicle data processors in carring out data collection of exterior images in a standardized manner, and verify the effect of contour processing of the face and license plate part of exterior images. The Practice Guidance sets forth the procedures, methods and verification standards for verifying the effects of contour processing of the face and license plate part of exterior images outside of a vehicle.	6 January 2023	Practice Guidance (Draft for Comments)
Guidelines for Declaration Materials for Data Export Security Assessment in Zhejiang Province **浙江省数据出境安全评估申报材料指引**	In order to guide and help data processors to carry out data export security assessment and declaration formalities, the Zhejiang Provincial Internet Information Office provides further guidance on the requirements for the completeness of the application materials under the Data Export Security Assessment Measures and Data Export Security Assessment Declaration Manual (First Edition) ("**Manual**") in the Guidelines for Application Materials for Data Export Security Assessment in Zhejiang Province ("**Guidelines**"). The Guidelines sets out the following requirements: 1. there must not be any missing items in submission documents; and the content therein must be complete; 2. information disclosed must be true and accurate, translation of the documents must be accurate and reports/legal documents must be valid; and 3. formatting, content and sequence of the submission documents must be consistent with the that of the template contained in the Manual.	6 January 2023	Provincial Guidelines for Security Assessment for Data Export

Development	Summary	Date	Links
Circular of the Ministry of Industry and Information Technology on Further Improving Mobile Internet Application Service Capabilities **工业和信息化部关于进一步提升移动互联网应用服务能力的通知**	The Ministry of Industry and Information Technology ("**MIIT**") has recently issued the Circular on Further Improving Mobile Internet Application Service Capabilities ("**Circular**"). The Circular prescribes for further improvement of mobile internet application service capabilities by regulating app installation and uninstallation, optimizing service experience, and strengthening personal information protection, for which 12 measures are set forth, three relating to app installation and uninstallation, including: 1. ensuring informed consent for installation and not misleading by a false name or otherwise deceiving users into downloading or installing an app; 2. regulating recommended downloads on webpages, prohibiting automatic or mandatory downloads without consent or voluntary choice by users when they browse a webpage; and 3. enabling easy installation, ensuring that an app can be easily uninstalled except basic functional software. The Circular also establishes a set of measures aimed at optimizing service experience and strengthening personal information protection. Apps are required to reasonably request permissions and to inform users of the purpose of any permission requested at the same time when it dynamically requests permissions when activated, especially if it requests to access photo album, address book, location or like data.	6 February 2023	New Regulation
Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information **个人信息出境标准合同办法**	The Cyberspace Administration of China ("**CAC**") recently issued the Measures on the Standard Contract for the Outbound Transfer of Personal Information ("**Measures**") with a template standard contract ("**Standard Contract**"). The Measures will take effect on 1 June 2023, but will allow a 6-month grace period. Consequently, from 1 December 2023, at the latest, an entity or person outside the PRC may need to sign the Standard Contract to get personal information from its subsidiaries, associated companies or partners in China, or to access personal information stored within China.	Promulgation date: 22 February 2023 Effective date: 1 June 2023	China SCCs

Development	Summary	Date	Links
	According to the Measures, the PRC personal information processors must meet all of the conditions below in order to provide the personal information abroad using the Standard Contract: 1. it is not a critical information infrastructure operator ("**CIIO**"); 2. it processes the personal information of less than 1 million individuals; 3. it has cumulatively transferred abroad the personal information of less than 100,000 individuals since January 1 of the previous year; and 4. it has cumulatively transferred abroad the sensitive personal information of less than 10,000 individuals since January 1 of the previous year. As a mandatory security assessment is required when the personal information concerned exceeds any of the thresholds in items (ii), (iii) or (iv) above, the PRC data processors shall not use quantity splitting or similar methods to escape the security assessment. The key points under the Measures and the Standard Contract are set out as follows: 1. PRC personal information processors and overseas recipients may not amend the Standard Contract. However, they can agree on additional terms that do not conflict with the Standard Contract. For instance, the Standard Contract shall be governed by the laws of the People's Republic of China as per its Article 9, and thus the parties do not have a choice on the governing law. Any of additional terms shall be included in an appendix to the Standard Contract 2. the outbound transfer of personal information shall occur only after the effective date of the relevant Standard Contract. The Standard Contract shall be filed by the PRC personal information processor with the CAC for record within 10 working days from the date when it takes effect. The absence of filing, however, will not affect the validity of the Standard Contract		

Development	Summary	Date	Links
	3. the commencement date and expiry date of the personal information retention term by the offshore recipient shall be specified in the Appendix I of Standard Contract 4. the offshore recipient shall promptly notify the PRC personal information processor if it receives a request for the provision of the transferred personal information from a governmental authority or judicial authority in the country or region where the offshore recipient is located 5. the offshore recipient shall satisfy all conditions below to provide the transferred personal information to a third party outside China: i. there is a necessity from the business perspective; ii. the personal information subject shall be properly informed; iii. explicit consent of the personal information subject shall be obtained; iv. a written agreement shall be entered into with the third party to ensure that the processing of personal information by the third party meets the standards for the protection of personal information required by the PRC laws, and the offshore recipient will be liable for any infringement of the personal information subject's rights caused by the provision of transferred personal information to the third party; and v. a copy of the written agreement with the third party shall be provided to the personal information subject upon his/her request. 6. either party may terminate the Standard Contract if the offshore recipient violates the laws and regulations of the country or region it is located for performing the Standard Contract 7. the parties to the Standard Contract shall assume joint and several liability in accordance with the law, and the personal information subjects shall have the right to claim against either party or both parties for violations		

Development	Summary	Date	Links
	8. if the personal information subject exercises the rights as a third-party beneficiary with respect to a dispute under the Standard Contract, the personal information subject may file a lawsuit with a competent court in accordance with the PRC Civil Procedure Law Any person may report to the CAC if it finds any outbound transfer of personal information in violation of the Measures.		
Administrative Measures for Network and Information Security in Securities and Futures Industries **证券期货业网络和信息安全管理办法**	The China Securities Regulatory Commission has recently released the Administrative Measures for Network and Information Security in Securities and Futures Industries ("**Measures**"), which takes effect from 1 May 1 2023. The Measures focus on network and information security and set forth a clear path for implementing the upper-level laws in the securities and futures industries based on past practice and experiences. They cover various entities, ranging from securities and futures critical information infrastructure operators, core institutions and operating institutions, to information technology system service institutions. The Measures take security as the basic principle, and specify the norms and requirements for network and information security management, which mainly involve: network and information security operation, protection of investors' personal information, network and information security emergency response, security protection for critical information infrastructure, network and information security promotion and development, supervision and administration, as well as legal liability.	Promulgation date: 27 February 2023 Effective date: 1 May 2023	Administrative Measures for Securities and Futures Industries
Information Security Technology—Certification Requirements for Cross-border Transmission of Personal Information (Draft for Comments) **信息安全技术** **个人信息跨境传输认证要求（征求意见稿）**	The National Information Security Standardisation Technical Committee ("**NISSTC**") has issued the Information Security Technology—Certification Requirements for Cross-border Transmission of Personal Information (Draft for Comments) ("**Draft**"), which is open to public comment until 15 May 2023. The Draft aims to address the issue of clarifying the relevant security requirements for cross-border processing of personal information, to underpin the requirement for "establishing a certification system for personal information protection" as set forth in Article 38 of the Personal Information Protection Law of the PRC. The Draft lays down the basic principles and	16 March 2023	National Standard (Draft for Comments)

Development	Summary	Date	Links
	requirements for cross-border provisions of personal information by personal information processors. Its overall structure and main content consist of seven parts, including the scope, normative references, terms and definitions, abbreviations, basic principles, basic requirements (including having legally binding agreements, organizational management, rules for cross-border processing of personal information, personal Information protection impact assessment) and protection of the rights and interests of personal information subjects (including the rights of personal information subjects, the responsibilities and obligations of personal information processors and overseas recipients).		
Provisions on the Administrative Law Enforcement Procedures of Cyberspace Authorities 网信部门行政执法程序规定	The CAC has published the Provisions on Administrative Law Enforcement Procedures of Cyberspace Administration ("**Provisions**"). The Provisions outline the procedures for the administrative supervision of enforcement actions for violations of applicable data protection and security regulations. Further, the Provisions stipulate the procedures for investigation and evidence collection by cybersecurity and informatisation departments, and the different situations for handling violations of data protection and security regulations. The key requirements of the Provisions are summarised as follows: 1. prior to the imposition of administrative penalties, cybersecurity and informatisation departments must notify parties concerned of their right to request a hearing, and that they must make such a request within five days of receiving a notification; 2. Should a party fail to request a hearing within the five-day TIMEFRAME, the party will have waived its right to a hearing, and may be subject to: i. a relatively large fine; ii. confiscation of relatively large amounts of illegal income and relatively large-value illegal property; iii. the lowering of qualification levels and the revocation of licences;	Promulgation date: 18 March 2023 Effective date: 1 June 2023	Provisions Regarding Administrative Enforcement

Development	Summary	Date	Links
	iv. orders to stop production and business to close down or restrict business operations; v. other heavier administrative penalties; and vi. other circumstances stipulated by laws, administrative regulations, and departmental rules. 3. before making a decision on administrative enforcement procedures, the cybersecurity and informatisation departments must inform the parties involved of the proposed administrative enforcement decision, the facts, reasons, and basis for the decision; and 4. parties in financial difficulties may apply for an extension or payment of fines in instalments, and where parties fail to pay administrative penalties within the time limit, an additional 3% of the total amount will be imposed daily.		

Czech Republic

Contributors

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

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

Development	Summary	Date	Links
The European Commission lawsuit against Czechia for failure to implement Whistleblowing Directive	The European Commission referred the Czech Republic to the Court of Justice for failing to implement the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law. The Directive requires Member States to provide whistle-blowers working in the public and private sectors with effective channels to report breaches of EU law confidentially, and to establish a robust system of protection against retaliation. Member States had to implement the necessary measures by 17 December 2021. The Czech Ministry of Justice stated that it is realistic to expect the Bill to be adopted by the Parliament later this year. The Bill is currently before its second reading in the Chamber of Deputies.	15 February 2023	Infringement procedure Bill
New guidance of the Office for Personal Data Protection on Cookie bars and granting consent	On 7 March 2023, the Office for Personal Data Protection (the "**Office**") published new guidance for Personal Data Protection on Cookie bars and granting consent. The Electronic Communications Act distinguishes between 2 types of cookies: 1. "technical cookies" are necessary for the actual operation of the website 2. "non-technical cookies" are designed for marketing purposes If a website only uses technical cookies, there is no need to implement a cookie bar; however, it is still necessary to abide by the GDPR information obligation. Conversely, non-technical cookies can only be activated after an explicit consent of the visitor has been given. In particular, the Office stated the following:	March 2023	Guidance

Development	Summary	Date	Links
	1. the cookie bar must not prevent interaction with the website even if the visitor has not yet selected any of the options; 2. access to services must not be made conditional on consent (cookie wall); 3. pre-ticked "YES" boxes do not constitute a consent; 4. consent may be withdrawn at any time; 5. the "refuse" button must be positioned in such a way that any consent given is free from coercion and the visitor is not misled; and 6. if the cookie bar can be closed without any option being selected, closing the bar and remaining on the website cannot be considered as a consent. The Office considers 12 months to be a reasonable period of time for which consent can generally be retained. However, if the user has refused to give consent, consent should not be required again for at least 6 months from the last time the cookie bar was viewed.		
New Act on Certain Measures Against the Dissemination of Terrorist Content Online	The Act on Certain Measures Against the Dissemination of Terrorist Content Online ("**Act**"), which takes effect on 30 March 2023, builds on the directly applicable Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. The Act provides that if a police anti-terrorism unit finds that hosting services are being misused to publicly disseminate terrorist content online, it may issue an order to remove the terrorist content or prevent access to it. The Czech Telecommunications Office will monitor the measures introduced by hosting service providers, as well as address offences. The fine imposed on hosting service providers may be as high as CZK 100,000 (approx. EUR 4,200) or CZK 200,000 (approx. EUR 8,400) for certain offences. Higher fines may also be imposed for persistent or long-term violations.	30 March 2023	Act

Germany

Contributors

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

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

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

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

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

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

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

Development	Summary	Date	Links
Too indefinite consent clause in e-mail advertising is invalid	The accused company offered consumers the opportunity to sign up for its customer loyalty program. After registration, customers received personalized newsletters and general newsletters. The consent form explicitly referred to the storage, processing and use of the customer's e-mail address for advertising purposes. According to the Higher Regional Court of Hamm, it is not evident from this that the consent relates to the receipt of personalized newsletters as part of the customer loyalty program on the one hand and to the receipt of general	3 November 2022	Court decision in German

Development	Summary	Date	Links
	newsletters on the other. The court decision states that the division must be clearly set out in the consent form.		
Credit agencies may keep insolvency data longer than official insolvency notice portal	The Munich Higher Regional Court has ruled that credit agencies (in Germany, Schufa in particular) may retain data on a remaining debt discharge in their database for longer than the official insolvency notice portal. The six-month period does not apply to credit agencies.	29 November 2022	Court decision in German
Cookie banner unlawful if option to reject is not highlighted in the same way as acceptance options	The Munich I Regional Court has ruled that the cookie banner of a major German media platform is unlawful. The main options were to "accept" the cookies and to open the "settings". Under settings, it was possible to choose between "Accept all", "Save selection" or "Reject all". However, the option to completely reject was only written in pale font and was not located directly next to the other two options. The court assumed that the user's consent was therefore invalid.	29 November 2022	Court decision in German
Data subject has right to choose data protection appeal with local jurisdiction	The High Administrative Court of Kassel has ruled that a data subject has the right to choose the local jurisdiction of the court when filing an action under data privacy law. It can decide between its own habitual residence or the registered office of the controller. This follows from Sec. 44 BDSG, which supplements the GDPR in this regard.	1 December 2022	Court decision in German
Court decides employee monitoring in logistics center of international e-commerce company is lawful	At a German logistics center of an international e-commerce company, hand movement scanners are used on employees to accurately record specific work steps. The company also uses the collected data to create quantity and quality performance profiles as well as for feedback discussions and process analyses. The Lower Saxony State Commissioner for Data Protection considered this to be illegal and issued a prohibition order. The company took legal action against this, justifying the measures in particular on the grounds of legitimate interest in data processing. The Hanover Administrative Court ruled in favor of the company, as the court found that the data processing can be based on Article 88 (1) of the GDPR in conjunction with Section 26 (1) sentence 1 of the German Federal Data Protection Act (BDSG).	9 February 2023	Court decision in German

Development	Summary	Date	Links
Coordinated audit on the position and duties of data protection officers	The Supervisory Authority of Bavaria (BayLDA) participated in a joint review of data protection supervisory authorities. This marks the start of the second Europe-wide review of the European data protection supervisory authorities, which focuses on the position and tasks of data protection officers.	15 March 2023	Press release in German

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

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

Kelvin Ng
Trainee Solicitor
kelvinng@
eversheds-sutherland.com

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

Development	Summary	Date	Links
Conviction against Chinese medicine practitioner in a direct marketing case	Hong Kong Courts have convicted a Chinese medicine practitioner of two charges of direct marketing offences under the Personal Data (Privacy) Ordinance ("**PDPO**") upon her guilty plea. The case originated from a complaint received by the Privacy Commissioner for Personal Data ("**PCPD**") in late 2020. The complainant was a patient of a Chinese medicine clinic which the defendant formerly worked at. During her employment with the clinic, the defendant never provided consultation to the complainant. In December 2020, the complainant received a WhatsApp message from the defendant, claiming to be a former	10 February 2023	Media Statement

Development	Summary	Date	Links
	Chinese medicine practitioner at the clinic. In that message, the defendant circulated her business card in an attempt to promote the Chinese medicine service of her new clinic. Pursuant to section 35C(1) of the PDPO, a data user who intends to use a data subject's personal data in direct marketing shall take certain specified actions, including but not limited to providing sufficient information (such as types of data and classes of goods/services to be advertised) and obtaining consent. As further provided in section 35F(1) of the PDPO, a data user is required to inform the data subject of his/her right to request cessation of the data use upon initial direct marketing. After the complaint was lodged, the PCPD referred the case to the Police for criminal investigation, who subsequently laid charges in October 2022. The defendant was fined HK$2,000 for each charge, amounting to a total of HK$4,000 in February 2023.		
Privacy Commissioner for Personal Data briefs Legislative Council panel members on PCPD's work in 2022	The Privacy Commissioner for Personal Data attended the Legislative Council Panel on Constitutional Affairs on 20 February 2023 to brief its members on the work of the Office of the Privacy Commissioner for Personal Data ("**PCPD**") in 2022 and its strategic focus in 2023. A report on the work was issued for this purpose. Looking back on the previous year, the PCPD reported that, from the implementation of the Personal Data (Privacy) (Amendment) Ordinance 2021 (on 8 October 2021) to the end of 2022, the PCPD initiated 114 criminal investigations and made 12 arrests. Amongst others, it also reported on its promotion, publicity and public education efforts, as well as its engagement in the privacy protection community at regional and international levels. As for the way forward, the PCPD has identified data security and cybersecurity as one of its strategic focuses in 2023 in light of increased digitalisation of data and the upward trend in cyberattacks and data breaches. Enhanced enforcement is another focus for the PCPD in the coming year – this includes continuous and close monitoring of doxxing activities, timely and effective enforcement actions on all fronts, and heightening public awareness through publicity and education to combat doxxing acts.	20 February 2023	Report

Development	Summary	Date	Links
	Importantly, another key highlight of PCPD's strategic focus in 2023 is to formulate a concrete legislative proposal to amend the Personal Data (Privacy) Ordinance ("**PDPO**"). The proposed amendments include establishing a mandatory data breach notification mechanism, requiring formulation of a data retention policy, empowering the PCPD to impose administrative fines, and introducing direct regulation of data processors. This proposal aligns with the Paper on the Review of the PDPO published by the Legislative Council Panel on Constitutional Affairs in early 2020. The Government and the PCPD's target is to consult the Legislative Council Panel on Constitutional Affairs on the specific legislative proposals concerning the Ordinance in the second quarter of this year.		
Hong Kong Courts hand down second sentence for doxxing offence	Hong Kong Courts have handed down a second sentence in respect of the new doxxing offence. This is the second sentencing case prosecuted by the Office of the Privacy Commissioner under the new anti-doxxing regime, which took effect on 8 October 2021. The case concerns the falling out of a business relationship between an online trader (the defendant) and its supplier (the complainant). Following a monetary dispute between the parties, the defendant disclosed the personal data of the victim and her husband on various social media groups. The personal data included the Chinese names and photos of the complainant and her husband, and the phone number of the complainant. Pursuant to section 64(3A) of the Personal Data (Privacy) Ordinance ("**PDPO**"), it is a criminal offence to disclose personal data of a data subject without the relevant consent, provided the said disclosure was made with an intent to cause specified harm or a person was reckless as to whether specified harm would be caused to the data subject or their family member. As highlighted in our previous updates, caution should be exercised given the broad definition of "specified harm", ranging from bodily or psychological harm to harm causing reasonable concern for a person's safety or well-being. The defendant was ultimately convicted of 14 charges under the new doxing offence upon her guilty plea, and was sentenced to two-month imprisonment, which was suspended for two years.	8 March 2023	Media Statement

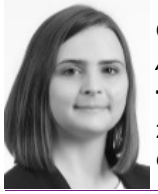
Hungary

Contributors

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

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

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



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

Development	Summary	Date	Links
A new law has been promulgated which introduces the transparency authority procedure among the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information	The purpose of the new legal instrument is to enforce the obligation for certain public bodies (with the exception of the national security services) to publish specific management information on the newly created Central Information Public Data Register (https://kif.gov.hu/) on a bi-monthly basis. The transparency procedure may be compelled by the Hungarian National Authority for Data Protection and Freedom of Information ("**NAIH**") on the basis of a notification or ex officio if the public bodies subject to the publication obligation fail to comply. The time limit for its administration is 45 days. The NAIH, acting in its official capacity, may by decision establish the existence of a breach of the publication obligation, including where the publication has been made with inaccurate or incomplete information, and in this context order the publication obligation (including the publication of accurate information, the filling in of missing information) to be fulfilled within a maximum of 15 days. If the public body fails to comply with the decision within the deadline, the NAIH may impose a fine ranging from HUF 100,000 to HUF 50 million.	28 February 2023	Legal instrument

Development	Summary	Date	Links
	The NAIH will take into account all the circumstances of the case when deciding whether it is justified to impose a fine in the framework of the transparency procedure and when determining the amount of the fine. The NAIH may also order the publication of its decision by publishing the details of the person subject to the disclosure obligation. As a background rule for the transparency authority procedure, Act CL of 2016 on the General Administrative Procedure applies. The above provisions entered into force on 28 February 2023, in line with the start of the obligation to publish on the interface of the Central Public Information Register.		

Ireland

Contributors

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

Ellie Cater
Senior Associate
T: +35 31 66 44 28 0
elliecater@
eversheds-sutherland.ie

Leona Chow
Solicitor
T: +35 31 66 44 25 8
leonachow@
eversheds-sutherland.ie

Julia Launders
Trainee
T: +35 31 66 44 97 8
julialaunders@
eversheds-sutherland.ie

Daire O'Herlihy
Trainee
T: +35 31 66 44 99 4
daireoherlihy@
eversheds-sutherland.ie

Development	Summary	Date	Links
DPC announces conclusion of two inquiries into social media provider	The Data Protection Commission ("**DPC**") fined a leading social media provider €210 million for breaches of the GDPR relating to one of its service offerings and €180 million for breaches in relation to a second service, after receiving the European Data Protection Board's ("**EDPB**") binding decision pursuant to the Art. 65 GDPR dispute resolution procedure. The inquiry examined complaints made about to the social media provider's updates to their Terms of Use in advance of the introduction of the GDPR, including reliance on 'contractual necessity' to justify processing conducted in connection with its online behavioural advertising activities.	4 January 2023	DPC report
DPC announces conclusion of inquiry into messaging service	The DPC concluded its inquiry into a messaging provider in connection with the delivery of its service, in which it fined them €5.5 million for breaches of the GDPR (predominantly, related to transparency) relating to its service.	19 January 2023	DPC report

Development	Summary	Date	Links
	The inquiry concerned a complaint made by a German data subject about the change in the Terms of Service in advance of the introduction of the GDPR. Prior to this, the messaging provider informed users that if they wished to continue to have access to the messing service following the introduction of the GDPR, existing (and new) users were asked to click "agree and continue" to indicate their acceptance of the updated Terms of Service. The messaging service would not be accessible if users declined to do so.		
Circuit Court judgment stays proceedings pending CJEU Referral on non-material damage under GDPR	In a recent Circuit Court judgment, *Cunniam v Fastway Couriers Dublin, Circuit Court Record No. 2021/03424*, the Court concluded that "*justice is best served*" by granting a stay of a data subject's damages claim pending determination of certain preliminary references currently before the CJEU. The Court expressed a view that damages in the case, if awarded, were likely to be small and a stay would not impact the procedural efficiency of the proceedings, but a delay in granting a stay could substantially and unnecessarily increase legal costs for the defendant. The judgment is significant because it not only has an impact on existing or potential plaintiffs in relation to this particular incident, but also is clearly relevant to other data subject damages claims generally in the pipeline where the claim is for non-material loss 'suffered' in relation to the processing of personal data.	23 January 2023	Judgment
DPC fines Centric Health Ltd	The DPC fined the medical group Centric Health Ltd €460,000 as a result of the inadvertent destruction of approximately 2,500 patient files and other data deletions following a ransomware attack. The decision of the DPC focused on whether Centric Health Ltd complied with Articles 5(1)(f) and 32(1) of the GDPR.	23 February 2023	Inquiry Decision
DPC publishes Annual Report for 2022	The DPC published its Annual Report for 2022 ("**Report**"). The Report provides an insight into the work of the DPC during 2022. It includes key areas of interest that the DPC has identified and information on the number of data breaches, complaints, enquiries, etc. received by the DPC during 2022. The most	7 March 2023	Overview Report

Development	Summary	Date	Links
	frequent GDPR queries and complaints received by the DPC related to access requests; fair processing; disclosure; direct marketing; and the right to be forgotten.		
Eversheds Sutherland Ireland article on the DPC publishing its Annual Report for 2022	This article summarises some initial key areas of interest from the Report. 2022 marked the fourth full year of the implementation of the GDPR and saw significant effort by the DPC to ensure compliance with the GDPR and applicable national legislation (the Data Protection Act 2018; the ePrivacy Regulations 2011; and the Data Protection Acts 1988-2003) across Ireland. Helen Dixon, Data Protection Commissioner for Ireland, highlighted that "2022 was a year that saw significant outputs from the DPC in its efforts to drive GDPR compliance and protect the rights of those in Ireland and across the EU." This is reflected in the statistics highlighted in the Report.	7 March 2023	Eversheds Sutherland article

Italy

Contributors

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

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

Development	Summary	Date	Links
IDPA provided indications on the interpretation and application of the provisions of legislative decree 104/2022 which are relevant for a data protection standpoint	On 13 August 2022, Legislative Decree No. 104/2022, implementing Directive (EU) 2019/1152 of the European Parliament and of the Council of 20 June 2019 on transparent and predictable working conditions in the European Union ("**Transparency Decree**") came into force. Inter alia, the Transparency Decree introduced information obligations for employers if they use "automated decision-making or monitoring systems deployed to provide indications relevant to the recruitment or appointment, management or termination of the employment relationship, assignment of tasks or duties as well as indications affecting the monitoring, evaluation, performance and fulfilment of contractual obligations of employees". Due to data protection law implications, and in response to the several doubts raised by public administrations and companies, the IDPA published and made available with its newsletter dated 24 January 2023, its "Interpretative and applicative data protection issues related to the entry into force of Legislative Decree no. 104 of 27 June 2022 on transparent and predictable working conditions" ("**Indications**"): 1. In its Indications, IDPA specified some elements to be taken into account in the case of processing that falls under the Transparency Decree regarding: i. Subjective scope of application; ii. Legal basis; 2. Information on the employment relationship; 3. Risk analysis;	24 January 2023	IDPA indications on the interpretation and application of the Transparency Decree (Italian only)

Development	Summary	Date	Links
	4. Privacy by design and by default; and 5. Records of processing activities.		
IDPA fined three regional health authorities for the use, without appropriate legal basis, of algorithms data aimed at analysing and predicting the evolution of patients' health conditions	The IDPA fined three regional health authorities ("**ASL**") that, using algorithms, had classified patients in relation to the risk of having or not having complications in the event of a Covid-19 infection. The ASLs had processed the data stored in their databases in order to initiate appropriate medical interventions towards the patients and identify the most appropriate medical treatments in time. During the preliminary investigation, the IDPA found that the data of the patients had been processed in the absence of an appropriate legal basis, without providing the data subjects with all the necessary information (in particular, on the means and purposes of the processing) and without having first carried out a Data Protection Impact Assessment required by GDPR. The IDPA stressed that the profiling of patients, resulting in the automated processing of personal data aimed at analysing and predicting the evolution of their health conditions and the possible correlation with other elements of clinical risk, can only be carried out in the presence of an appropriate legal basis, in compliance with specific requirements and adequate guarantees for the rights and freedoms of the data subjects, which were lacking in this case. Thus, having ascertained the violations and assessed that in this specific case the operations, using algorithms, had concerned the health data of a large number of patients, the IDPA fined each of the three ASLs EUR 55.000 and an obligation to delete the processed data.	Date of IDPA's Newsletter n. 499, making available IDPA's measures: 24 January 2023 Date of IDPA's measures n. 415, n. 416, and n. 416: 15 December 2022	IDPA's newsletter 499 of 24 January 2023 (Italian only) IDPA measure n. 415 of 15 December 2022 (Italian only) IDPA measure n. 416 of 15 December 2022 (Italian only) IDPA measure n. 417 of 15 December 2022 (Italian only)
Publication of IDPA's six-months investigation plan (January - June 2023)	The IDPA published its investigation plan for the period from January to June 2023. The inspection activity performed by the IDPA (either directly or availing of the specialized Italian Tax Police) is addressed to cover:	26 January 2023	IDPA measure of 26 January 2023 - six-months investigation plan for the period January-June 2023 (Italian only)

Development	Summary	Date	Links
	1. As a priority, the completion of the inspection activities already started during the second half of the year 2022, with particular regard to: i. audits on digital identity providers and service providers using digital IDs (also for professional use or for minors) in the context of online services also offered through apps by public administrations; ii. checks on the proper implementation of IDPA's 2021 Guidelines on cookies and other tracking tools, also availing of online assessments; and iii. continuation of audits on the processing of personal data through telemarketing activities and loyalty cards; 2. Other inspections of public and private entities, in order to verify compliance with the provisions on the protection of personal data, including investigations relating to formal complaints and reports submitted to the IDPA and under investigation by the relevant Departments and Services. The above is without prejudice to the fact that IDPA may perform further investigations both ex officio and following reports or complaints.		
IDPA ordered to a US IT provider the provisional restriction of its processing of personal data of users in the Italian territory performed by using an AI-based chatbot	The Italian Data Protection Authority ("**IDPA**") ordered a US IT provider to restrict the processing of personal data of users in Italy through an AI-based chatbot - equipped with a written and vocal interface that relies on artificial intelligence to generate a "virtual friend"- due to the associated risks for minors. The IDPA found that this chatbot answered questions posed by children with answers incompatible with their age, has characteristics that may increase risks for vulnerable individuals still in a developmental stage or in a state of emotional fragility and lacks any age verification mechanism in the account creation phase. The IDPA declared that the chatbot breaches GDPR ass it does not respect the principle of transparency, and performs unlawful processing of personal data (which cannot be based, even	2 February 2023	IDPA's measure n.39 of 2 February 2023

Development	Summary	Date	Links
	implicitly, on a contract that the minor is incapable of concluding).		
IDPA fined an Italian operator of the energy sector on the account of unlawful data processing for telemarketing purposes	Following several complaints, the IDPA investigated an Italian operator in the energy sector and found several data protection law infringements: 1. performance of marketing telephone calls without the addressees' consent; 2. failure to respond to the objection to unsolicited telephone calls; 3. impossibility for data subjects to provide free and specific consent in a granular way for the various purposes sought (promotional, profiling, communication of data to third parties) within the website or app; and 4. provision of incomplete or inaccurate privacy notice. The IDPA ordered the operator: 1. to facilitate the exercise of data subjects' rights and to provide feedback, without delay, to requests, including those relating to the right to object. In particular, the IDPA explicitly stated that the addressee can object to unsolicited marketing calls at any time, including during the call, without need for confirmation by e-mail or other means, and that this objection is also valid for future promotional campaigns. In the event of an objection, the call centre or company must immediately stop making other calls; 2. not to perform processing activities for marketing purposes using contact lists prepared by other companies that have not acquired a free, specific, informed, and documented consent to the communication of user data, prescribing the operator; 3. in case of marketing campaigns addressing contact lists provided by third parties, to always verify, also by means of adequate sample checks, that personal data is processed in full compliance with data protection laws;	Date of IDPA's newsletter 500 of 21 February 2023, making available IDPA's measure: 2 February 2023 Date of IDPA's measure n. 431: 15 December 2022	IDPA's newsletter 500 of 21 February 2023, making available IDPA's measure (Italian only) IDPA's measure n. 431 of 15 December 2022 (Italian only)

Development	Summary	Date	Links
	4. not to process data for marketing and profiling purposes collected without free and specific consent; and 5. to provide data subjects with correct information, indicating only the processing activities actually carried out. In light of all the above, the IDPA fined the energy operator EUR 4,9 million.		
Legislative Decree No. 24 of 10 March 2023 implementing in Italy Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national law	On 15 March 2023, the Legislative Decree No. 24 of 10 March 2023, providing for the "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 ("**Directive**") on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national law" ("**Decree**") was published in the Italian Official Journal. In the implementation of the Directive, which aims to harmonise the regulations on whistleblowing in the various Member States, the Decree brings together the relevant provisions in a single regulatory text, providing for minimum standards of protection and the introduction of greater guarantees to protect whistle-blowers, both in the public and private sectors. The Decree regulates the protection of persons who report violations of national or European Union law that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private work context. Some of its provisions have data protection significance: 1. **Internal reporting channels**: these must guarantee, also through the use of encryption tools, the confidentiality of (a) the identity of the reporter; (b) the identity of the person involved; (c) the identity of the person mentioned in the report; (d) the content of the report and the relevant documentation; 2. **Reports**: they may not be used beyond what is necessary to adequately follow them up. In this regard, the Decree identifies a retention period, providing that "reports, internal and external, and the related documentation shall be	Date of applicability of the Decree: 2 February 2023 Date of applicability of the Decree In case of private sector entities that have employed, over the past year, an average of up to 249 employees, under permanent or term-based employment contracts: 17 December 2023	Legislative Decree 24/2023 (Italian only)

Development	Summary	Date	Links
	retained for the time necessary to process the report and, in any event, no longer than 5 years from the date of communication of the final outcome of the reporting procedure". 3. **Consent**: the identity of the reporting person and any other information from which their identity may be inferred, directly or indirectly, may not be disclosed without the express consent of the reporting person. 4. **Persons in charge of processing**: the persons in charge of handling reports must be authorised to process such data in accordance with the GDPR and the Italian Privacy Code. 5. **Processing**: the processing performed in the event of a report must comply with the principles and the several obligations under the GDPR.		
IDPA fined a messaging service company for illegally storing the content of text messages sent by its customers	The IDPA found a messaging services company in breach of data protection laws on the account of unlawful storage of the content of text messages sent by its customers (about 7,250 users). The company was also charged with other unlawful conduct relating, in particular, to the measures taken to ensure the security of the processing of telematic traffic data and the absence of a legal basis for carrying out anti-fraud checks. During the inspections, the IDPA found that the full content of messages sent by customers was stored without their explicit consent. Among the content of the messages, mostly consisting of service communications sent by users of the platform (banks, insurance companies, health companies,) to their customers, were also passwords to operate banking services (Otp - One time password), authentication credentials, and data relating to special categories (health status or political party membership). The contents of the text messages could also be accessed by the company's employees. The company justified its activity by arguing that the content of the text messages was part of traffic data, with a consequent obligation to retain them. In this regard, the IDPA recalled that no law requires the retention of the contents of communications, which, on the	Date of IDPA's newsletter 501, making available IDPA's measure: 2 February 2023 Date of IDPA's measure n. 12: 11 January 2023	IDPA's newsletter 501 of 15 March 2023, making available IDPA's measure (Italian only) IDPA's measure n. 12 of 11 January 2023 (Italian only)

Development	Summary	Date	Links
	contrary, is expressly prohibited unless authorised by the user with specific and free consent for the provision of value-added services. In addition, several other violations emerged in the course of the inspection activities, such as: 1. the retention of traffic data without a distinction between data retained for crime prevention and justice purposes and data retained for other purposes (billing or consultation by the customer); and 2. the lack of a distinction in data retention periods according to purpose. The IDPA also noted that the company performed prior automated checks, for anti-fraud purposes, on the content of text messages sent by its customers, to prevent possible phishing activities, but without having a suitable legal basis for doing so. The IDPA took into account the corrective measures adopted by the company in the course of the investigation proceeding, but anyway admonished the company for the violations found and issued a fine of EUR 80.000.		
IDPA fined a company that after the termination of a collaborator had kept her e-mail account active, viewing its content and setting up a forwarding system to another employee of the company	The legitimate interest in processing personal data to defend a right in court does not justify the restriction of employees' data protection rights, in particular if it affects a form of correspondence, whose secrecy is also protected under the Italian Constitution, such as e-mail messages. The IDPA found that a company, after the termination of the relationship with a collaborator, had kept her e-mail account active, viewing its content and setting up a forwarding system to another employee of the company. This collaborator, before the termination, had collected, on behalf of the company itself and via an e-mail account assigned for this purpose, the contact details of potential customers she had met at a trade fair. According to the company, her subsequent attempt to contact these potential customers on her behalf had subsequently led to a legal dispute.	Date of IDPA's newsletter 501, making available IDPA's measure: 2 February 2023 Date of IDPA's measure n. 8: 11 January 2023	IDPA's newsletter 501 of 15 March 2023, making available IDPA's measure (Italian only) IDPA's measure n. 8 of 11 January 2023 (Italian only)

Development	Summary	Date	Links
	Fearing losing opportunities with potential customers, the company had not only written to explain to them that the person had been removed but had also viewed their communications. According to the IDPA, neither the need to maintain relationships with customers nor the interest in defending one's own right in court legitimised such processing of personal data. In order to achieve an appropriate balancing of the interests at stake (the need to continue the economic activity of the controller and the right to privacy of the data subject), it would have been sufficient to activate an automatic reply system, with the indication of alternative addresses to be contacted, without viewing the inbound communications to the account. During the proceedings, it also emerged that the company, as data controller, had failed to both provide the data subject with an appropriate response to the request for deletion of the e-mail account and with an appropriate privacy notice. The IDPA deemed irrelevant the lack of formalization of an employment relationship since the obligation to inform the data subjects is an expression of the general principle of fairness. The IDPA fined the company EUR 5.000.		
Legislative Decree No. 26 of 7 March 2023 Implementing Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules	On 18 March 2023, the Legislative Decree 26/2023 ("**Decree**") implementing EU Directive 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council relating to the better enforcement and modernisation of Union consumer protection rules ("**Omnibus Directive**") was published in the Official Italian Journal. This Decree amends some provisions of Legislative Decree No 206/2005 (bringing the Italian Consumer Code). Some amended provisions are relevant from a data protection standpoint. **Personal data as payment:** The Decree provides that certain rules of the Italian Consumer Code (on information obligations, right of withdrawal, delivery obligations, means of payment, fees for communicating with the professional, supplementary payments, and administrative and judicial protection of the consumer) also apply in relation to	Date of applicability of Decree: 2 February 2023 Date of applicability of Decree's provision establishing the criteria for the identification of the so-called "previous price" for price reduction announcements: 1 July 2023	Legislative Decree 26/2023 Legislative Decree 26/2023 (Italian only)

Development	Summary	Date	Links
	contracts in which the professional provides the consumer with digital content by means of a non-material medium or a digital service, and the consumer provides or undertakes to provide personal data to the professional, unless the personal data provided by the consumer is only processed for the purpose of providing the digital content or the digital service and for no other purpose. **Targeting and price customisation:** The Omnibus Directive introduced the possibility for professionals to tailor the price of goods in relation to the characteristics of individual consumers or groups of consumers on the basis of automated decision-making and consumer behaviour profiling processes that allow professionals to assess the purchasing power of individual consumers. This possibility is accompanied by a duty for the professional. Consumers must, in fact, always be informed that the price offered is the result of an automated decision based on the processing of data concerning them. This provision touches on an extremely delicate issue, namely that of the processing of personal data and the automated decisions based on their processing. Recital 45, in fact, specifies that this possibility "shall be without prejudice to the provisions of Regulation (EU) 2016/679, which establishes, among other things, the right of natural persons not to be subject to automated decision-making regarding natural persons, including profiling". This possibility was also included in the Decree which, amending Article 49 of the Italian Consumer Code, provided that among the information that the professional must mandatorily disclose to consumers (in the context of distance contracts and off-premises contracts) the fact that the price has been customised on the basis of an automated decision-making process has to be included, without prejudice to the guarantees set forth in Article 22 of the GDPR. The professional will therefore still be required to comply with the data protection principles under the GDPR.		

Development	Summary	Date	Links
IDPA approves Code of Conduct on Telemarketing	The IDPA has approved the Code of Conduct for telemarketing and tele-selling activities promoted by associations of principals, call centres, telemarketers, list providers and consumer associations, pursuant to art. 40 GDPR. The Code will become effective once the accreditation phase of the relevant monitoring body will be completed, with the subsequent publication in the Italian Official Journal. The monitoring body is an independent body called upon to verify compliance with the Code of Conduct and to handle the resolution of complaints. To ensure compliance with privacy regulations "from contact to contract", companies adhering to the Code will undertake to adopt specific measures to guarantee the correctness and legitimacy of data processing carried out throughout the telemarketing chain. Adherents will have to collect specific consents for each purpose (marketing, profiling, etc.), inform contacted persons precisely about the purposes for which their data is being used, and ensure that they can fully exercise their rights under data protection law. Rules have also been introduced to counter the phenomenon of abusive call centres. The Code of Conduct provides that in contracts entered into by the operator with the service provider, a penalty or a non-payment of commission mechanism will have to be provided for each sale of service made as a result of promotional contact without consent. Companies will be required to carry out a Data Protection Impact Assessment if they carry out automated processing, including profiling, which involves a systematic and global analysis of personal data.	Date of IDPA's press release making available the Code of COnduct: 2 February 2023 Date of Code of Conduct (Code of conduct will become effective once the accreditation phase of the relevant monitoring body will be completed with subsequent publication in the Italian Official Journal).: 9 March 2023	IDPA's press release (Italian only) IDPA's measure n. 70 of 9 March 2023 bringing the Code of conduct (Italian only)

Netherlands

Contributors

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

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

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

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

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

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

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

Development	Summary	Date	Links
Data Subject request to erase Dutch Credit Registration Office (BKR) registration rejected	In these preliminary relief proceedings, the claimant requested to have BKR registrations and special codes removed from the Central Credit Information System (in Dutch: CKI). The claimant had an outstanding debt of €100.000 and had fallen behind on repayments. As a result, the claimant has been listed in the BKR register. The claimant argued that the BKR registration is no longer justified since he already met a number of the conditions	3 January 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	set by the bank for the repayment of the debt. The claimant invoked the right to have his personal data removed. **Assessment** The personal data registered includes personal data fields such as: name, address, date of birth and place of residence. It is only possible to remove the personal data procecessed if it is disproportionate or there is a less detrimental way to keep the register.. This means that it must be possible that less data of the data subject is processed in order to keep the register up to date, or that there is another way to process the data. The Court indicated that credit institutions can benefit from keeping the register and that they can demonstrate a necessity to request the information to keep the register up to date. In this case, there is no evidence that the registrations are based on an improper balancing of interests. The Court rejected the claimant's request to have the BKR registration removed.		
Claim for damages due to breach of privacy rejected	In the first instance, Infomedics claimed a conviction against the appellant for an unpaid medical care claim. In a counterclaim, the appellant claimed compensation from Infomedics for an infringement of her privacy. She also demanded that Infomedics destroy her medical file. The appellant had brought forward six grounds of appeal, in which she argued that the Court wrongfully ruled that the processing of personal data by Infomedics was lawful. The Court of Appeal does not follow the arguments of the appellant and ruled that Infomedics has lawfully and justifiably implemented the legal obligations of Article 38 paragraph 2 of the Health care (Market Regulation) Act by stating the medical care provided on the invoice and payment reminder. The fact that such information is used in Court proceedings is also considered lawful. The appellant's claim to have the medical file destroyed was also rejected because Infomedics had sufficiently proven that it does not possess the appellant's medical file.	10 January 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
The right of access, the right of rectification, the right to limit the processing of personal data and the notification obligation based on the GDPR are not transferable	The Court of The Hague has confirmed that the rights of data subjects are personal rights in a case in which the heirs of the deceased (A) want to take over their legal position. Before his death, A submitted a request for the rectification of his personal data processed by the Tax and Customs Administration and claimed damages. In addition, he also submitted a request for restriction of processing. He was of the opinion that more personal data was being processed than he had given access to. After the death of A, his heirs wanted to continue the proceedings. The claimants argued that the rights under GDPR, which A submitted before his death, were transferred to them by virtue of succession. The Court is primarily faced with the question of whether the appeals and the request for compensation are admissible. The Court first assessed whether the right of access, the right of rectification, the right to limit the processing of personal data and the notification obligation of the GDPR are transferable rights. The Court ruled that the rights of data subjects under the GDPR are personal rights, and that they are not transferable. Moreover, the rules from the GDPR do not apply to the personal data of deceased individuals. The claim for damages cannot be transferred to the heirs either, because this is a personal right. The Court therefore concluded that claimants cannot continue the proceedings.	24 January 2023	Court ruling (Dutch only)
Court rules that repeated applications of the same data subject request based on a different lawful basis under GDPR is unfounded	After assessing the claimant's appeal against the rejection of his application under Article 17 GDPR and his claim for damages of €1.000 due to a violation of his privacy, the Court dismissed the appeal as unfounded. In 2020, the claimant submitted a request to their local municipality to destroy all photographs of his home that were taken in 12 September 2012 as part of his objection to the assessment of the value of his home under the Property Tax Act. In addition, the claimant filed a request for damages. The claimant requested that he be awarded €1.000 because of the violation of privacy and domiciliary rights. This request was rejected by the Municipal Executive in May 2020.	24 January 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	In November 2021, the claimant served the Municipal Executive with a notice of default for failing to make a timely decision on the application contained in a letter from September 2020. In this letter, the claimant again requested the destruction of the photographs taken at his residence on September 21, 2012, referring to Article 17 GDPR and again requested compensation of €1.000. The Municipal Executive regarded the application as a repeated request and wanted to reject it on the basis of Article 4:6 of the General Administrative Law Act. The Court assessed whether the Municipal Executive had acted properly, carefully prepared, and properly substantiated their rejection; and whether there were any new facts or changed circumstances. The claimant did not present any new facts or changed circumstances and the Court ruled that the Municipal Executive did not violate the obligation to hear the claimant. The Court had no reason to doubt the authority of the secretary of the Objections Advisory Committee and the Municipal Executive complied with the legal requirements with regard to the decision. The argument of the claimant that the Municipal Executive failed to make clear how the decision was formed did not alter the outcome.		
DDPA statement: central database passport data poses high risk	The Dutch government aims to create a central database with all personal data provided by individuals by means of a passport application, such as fingerprints, signatures and passport photos. Such a database storing (sensitive) personal data from many Dutch individuals gives rise to privacy risks that the Dutch government has not yet properly considered. There may also be uncertainty regarding the party responsible for the security of the data. The DDPA therefore advises that the plans be amended significantly or otherwise withdrawn. At present, the municipality where an individual applies for a passport or identity card stores the necessary personal data locally in their own decentralized database. With an amendment to the Passport Act, the Dutch government now wants to change to one central database. Fingerprints would be stored in that database until the identity document is issued, passport photos and signatures are stored for a longer period of time.	30 January 2023	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	The DDPA points out that the Dutch government has therefore triggered a major privacy risk for Dutch citizens. While a central system may be more secure, their could be unintended consequences Having all the data in one place is a goldmine for cybercriminals, especially because it concerns sensitive biometric data. Instead of having to break into the databases of more than 300 municipalities, criminals will only have to break into one. Non-criminal related data breaches are also more severe with a central database, e.g. a data breach can cause far more sensitive personal data to be leaked compared to a breach occuring at a decentralised database. Moreover, such a central database creates the risk that the government will use the data for other purposes than issuing travel documents. The government does not substantiate why central storage is absolutely necessary. The risks and disadvantages are not properly mapped out and weighed against the interests and freedoms of individuals. Finally, the Dutch government does not distinguish the responsibility for the data storage in a clear manner. As a result, it is not clear who will be responsible for some of the processing activities.		
Data Subject's request to the erasure of personal data was rejected	In this case, the respondent had requested the erasure of his personal data processed by the foundation 'Safe at Home'. The Court ruled that the processing of the respondent's data by Safe at Home is lawful on the basis of a legal obligation under the Social Support Act 2015 and therefore rejected the request for the erasure of personal data. The Social Support Act 2015 arranges assistance and support for citizens so that they can live independently at home for as long as possible and continue to participate in society. The Court rules that Safe at Home is not obliged to delete the respondent's personal data pursuant to Article 17, paragraph 1(e) GDPR. The retention of personal data relating is not unlawful and above all necessary for the purpose for which Safe at Home had processed the personal data. In addition, the respondent has no right to erasure based on any other lawful basis under Article 17, paragraph 1 GDPR, because there are compelling legitimate grounds for the processing of the respondent's personal data.	03 February 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
Dutch Ministry of Justice and Security must immediately stop its large-scale processing of passenger name record data ("PNR-Data")	The Ministry of Justice and Security ("**Ministry**") must immediately cease its large-scale processing of Passenger Name Record data ("**PNR Data**"). The processing was initially intended to map out travel movements of terrorists and serious criminals. However, the travel details of all airline passengers are currently being collected and stored in a database for years. The DDPA determined this is not permitted and such processing activities must cease with immediate effect. With the processing of PNR data, a large amount of personal data is systematically collected, automatically processed and stored for many data subjects who do not belong to the group for which the database was originally intended. The necessity and proportionality of that processing cannot be justified. In 2022, the DDPA advised the Ministry to align the processing of PNR data with the legal frameworks and the European PNR Directive. Although the Ministry had not followed up on this advice, the DDPA refrained from enforcement pending legal proceedings before the CJEU. The DDPA found its conclusions confirmed in the ruling of the CJEU and concluded that enforcement is still necessary. The DDPA has established that its previous advice has not led to any action, or not enough. As a result, PNR data is processed unlawfully on a large scale. The Ministry will have to considerably limit the current processing to operations that are necessary and proportionate to combat terrorism and serious crime.	21 February 2023	DDPA Statement (Dutch only)
Tesla makes camera settings more privacy-friendly following DDPA investigation	Car manufacturer Tesla has made the settings of the built-in security cameras in vehicles more privacy-friendly. Tesla took these measures following an investigation by the DDPA. The DDPA investigated Tesla's so-called 'Sentry Mode'. Sentry Mode aims to protect the vehicle against issues such as theft or vandalism. This is done by taking pictures with 4 cameras on the outside of the vehicle. By default, when Sentry Mode is enabled, the cameras continuously recorded film footage of anything 'suspicious' surrounding a parked Tesla. It records 1 hour of footage each time.	22 February 2023	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	Tesla explained to the DDPA that the company made several adjustments since the investigation. The Sentry Mode now only becomes activated when the vehicle is touched and no longer records surroundings as soon as cameras see a 'suspicious' movement around the vehicle. In addition, the vehicle does not automatically start filming anymore. Instead, the owner receives a text message on the phone. The vehicle can still take camera images, but only when the user activates the function themselves. If the cameras are recording images, the vehicle will indicate this on the screen in the vehicle. The headlights also give a special light signal. This is how people know they are being filmed. Further, the vehicle saves 1 minute of footage as opposed to 1 hour of footage. However, the owner can increase this to 10 minutes total. The images are not shared with Tesla. The DDPA's investigation did not lead to a fine or other sanctions for Tesla. During the investigation, it was concluded that the owner of the vehicle is legally responsible (i.e. the data controller) for the images that the vehicle makes (not Tesla).		
Amsterdam District Court ruled that a social media provider violated privacy rights of users and unfair commercial practice laws	The ruling by the Amsterdam District Court concerned a class action that was recently brought before the Court under the old class action legislation. In the Netherlands, this is the first final judgment in a class action on the processing of personal data. The claimant represents the interests of Dutch users of the social media service. The core issue in these proceedings were whether the social media provider acted unlawfully in processing personal data of Dutch users in the period from April 1, 2010 to January 1, 2020. The Court had taken into account whether the social media provider processed personal data of users of the service not only to offer access to the social network, but also for advertising purposes. The Court found that the social media provider acted unlawfully towards those represented in the class action, due to violation of privacy rights and unfair commercial practice laws. There was no lawful basis for the processing and users were not properly informed regarding the processing. Key considerations:	15 March 2023	Court ruling (Dutch only)

Development	Summary	Date	Links
	1. Social media provider is considered data controller One of the issues concerned which one of the social media provider's entities qualified as a data controller for the relevant data processing within the meaning of the Personal Data Protection Act (the Dutch predecessor of the GDPR which was applicable between 2010-2018) ("**PDPA**") and the GDPR. The ruling concluded that only the Irish social media entity can be regarded as a data controller because it primarily determines the purpose and means for the processing of the personal data of Dutch users. In the opinion of the Court, the U.S and Netherland entities could not be considered joint controllers during the period between 2010-2020 as it was not clear for which concrete processing operations both entities would determine the means and purposes. **2. Provision of information requirements for specific processing operations** The claimant argued that the social media provider had not sufficiently informed users on the processing of personal data for advertising purposes in line with Article 33-34 PDPA and Article 12-14 GDPR. In this ruling, the Court applied a reversal of the burden of proof. The Court concluded that it follows from the PDPA and the GDPR that the social media provider had the burden of proving that it complied with its information obligations. Although this is less explicitly stated in the PDPA than in the GDPR, this follows from the transparency requirement since the data subject can only exercise their rights under GDPR if they are aware of the processing activities. Therefore, the controller must prove that the data processing is lawful. To that end, the data subject must be sufficiently informed in advance about the data processing. The Court concluded that the social media provider acted unlawfully by violating the information obligations with regard to four specific data processing operations. **3. Lawful basis for processing**		

Development	Summary	Date	Links
	Furthermore, the Court concluded that the social media provider did not have a lawful basis for the processing of personal data for advertising purposes. The lawful basis "necessary for the performance of the contract" (Article 6(1)(b) GDPR) must be strictly interpreted. The Court once again confirmed that the lawful basis "necessary for the performance of the contract" may not be extended, and cannot be used for processing for advertising purposes. Consent (Article 6(1)(a) GDPR) can only serve as a lawful basis if legally valid consent has been obtained. Requirements for valid consent include that it has to be freely given, specific, informed and unambiguous. When registering its users in the period between 2010 and 2020, the reading confirmation of the terms of use obtained by the social media provider cannot be considered a legally valid consent to the processing of personal data for advertising purposes. According to the Dutch Data Protection Authority ("**DDPA**"), a mere commercial interest cannot by definition serve as a legitimate interest (Article 6(1)(f) GDPR). The Court of Justice of the European Union ("**CJEU**") has yet to rule on the preliminary question of whether commercial interests can constitute a legitimate interest. The District Court does not exclude this possibility in advance. The social media provider has not demonstrated that there is legitimate processing for advertising purposes. In its statement, the social media provider did not expressly address the requirements of proportionality and subsidiarity. **4. Special category personal data** Under Article 16 of the PDPA and Article 9 of the GDPR, the processing of special category personal data is prohibited, subject to exceptions specified in law. The Court found that the social media provider also processed special category personal data, such as data on health and philosophical beliefs, for advertising purposes. The data was collected from the profile input fields filled in on a voluntary basis and derived from users' browsing behavior. The social media		

Development	Summary	Date	Links
	provider was not able to prove that it could rely on an exception to the prohibition of processing special category data. The fact that not every user filled in the profile input fields did not change the outcome that the processing is deemed unlawful. **5. Cookie tracking information and consent for the use of cookies** Another point of dispute relates to the question whether the social media provider had complied with the information and consent requirements with regard to tracking cookies that it placed on third-party websites to track the browsing behavior of users outside the service. According to the Court, the social media provider did not have a lawful basis for the processing of personal data obtained through the cookies. **6. Unfair Commercial Practices** Following the violation of privacy laws the Court also came to the conclusion that the social media provider engaged in unfair commercial practices and thus acted unlawfully during the relevant period. The Court ruled that the lack of information provided to the user, at the time of entering into the agreement, was a misleading omission of essential information necessary for the average consumer to come to an informed decision. The social media provider had not been sufficiently transparent on how preferences, personal data and user-generated content were used. The fact that the service is advertised as 'free' is not in itself misleading. However, the Court did state that the statement of being a 'free' service can play a role in assessing the lack of clarity about the business model. The causality will not be addressed, only when determining liability towards an individual consumer.		

Poland

Contributors

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

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

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

Development	Summary	Date	Links
Polish Data Protection Authority's sector control plan for 2023	The Polish DPA has published the sector control plan for 2023. Controls will focus on entities that process personal data using mobile applications and online (web) applications. Particular attention will be paid to the methods used by such entities to secure and share personal data processed in connection with the use of the applications. The scope of the planned inspections indicate that the DPA is particularly interested in the new technology, gaming and e-commerce industries.	18 January 2023	DPA Announcement (in Polish only)
The Polish DPA: personal data must be processed in a manner that ensures adequate security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage	The Polish DPA imposed an administrative fine on the Regional Court Szczecin-Center in Szczecin of PLN 30.000. The breach occurred due to the loss of three flash drive-type data storage devices: one company-encrypted and two privately-unencrypted. The lost storage devices contained draft rulings and justifications, with personal data included. The investigation established the long-standing use of private storage devices, unsecured and unverified by the court's IT department on business computer equipment. In addition, it turned out that the controller implemented only organizational measures in internal regulations to prohibit its	19 January 2023	DPA Decision (in Polish only)

Development	Summary	Date	Links
	employees from using private storage devices. Despite existing procedures the controller did not supervise whether court employees complied with internal regulations. The DPA in the course of the investigation found that the controller had not implemented adequate technical measures, such as blocking USB ports to prevent the use of private data storage devices. The DPA emphasized that the controller allowing the use of portable data storage devices should ensure that they are verified and registered by the IT department as well as encrypted and secured against unauthorized access in case they are lost or left unattended. Moreover the USB port should be blocked in order to prevent employees from using private storage devices to process personal data. The DPA emphasized that the implementation of technical and organizational measures by the controller is not a one-time activity, but should take the form of an ongoing process in which the controller reviews and, if necessary, updates previously adopted safeguards. A regular evaluation of the security measures in place would allow the controller to verify that the procedure put in place specifying the prohibition of the use of private storage devices is adhered to, and therefore effective. The DPA stated that if the controller had verified the implementation of the organizational measure in the form of a prohibition of the use of private storage devices, it would have then significantly reduced the risk of a breach or even led to its complete prevention.		
New legislation regarding remote work	On 7 April 2023, new regulations on remote work will come into force as part of an amendment to the Labour Code. Employers who intend to introduce remote work should take action, including drafting appropriate documents. One of the documents is a remote work agreement (if there are functioning trade unions) or remote work regulations (in the absence of trade unions). From the perspective of personal data, the development of a procedure for the protection of personal data in remote work is required, along with a statement from employees that they have familiarized themselves with such a procedure, as well as agree	27 January 2023	Amendment of the Labour Law on remote work (in Polish only)

Development	Summary	Date	Links
	to abide by it. The employer also gained the right to control the employee's remote work in relation to health and security. The new law also stipulates that if, during an inspection, violations are found in areas such as (but not limited to), compliance with information security and protection requirements, including procedures for the protection of personal data; then the employee shall be obliged to rectify the violations within the specified period, or the employer will be able to revoke permission for that employee to perform remote work. The new regulations also indicate that, where necessary, the employer should provide for employees instruction and training on data protection in remote work. For this reason, it should be verified whether the employer's existing training (e.g. onboarding) or recurring training includes in its scope the issue of data protection in remote work.		
New sobriety and drug control regulations in labour law	On 21 February 2023, as part of an amendment to the Labour Code, employers gained the right to conduct sobriety checks and for the presence of substances which have a similar effect to alochol (e.g. drugs). The scope of the control will extend beyond employees, and will also include persons employed under civil law contracts or cooperating with the employer in the course of business activities. In order to exercise this right, it will be necessary to establish the group or groups of employees covered by sobriety control, the manner of how the checks will be carried out, including the type of equipment used, the time and frequency of its conduct. The employer shall process information on the date, time, minute of the test, and the result of the test indicating a state of drunkenness or intoxication, only if it is necessary to ensure the protection of life and health of employees or other persons or the protection of property. The information stored on the employee's personnel file shall not be kept for a period exceeding one year from the date of its collection. Regarding the application of a warning, reprimand or fine, the employer shall keep information about the examination in the employee's personnel file until the penalty is declared non-existent, as per labor regulations. If the information contained in the results of the examination may constitute or constitutes	21 February 2023	Amendment of the Labour Law on sobriety and drug control (only in Polish)

Development	Summary	Date	Links
	evidence in a proceeding under the law, and the employer is a party to that proceeding or has become aware of the filing of a lawsuit or the initiation of a proceeding, the data retention period can be extended until the legal conclusion of the proceeding. Considering the nature of the right to conduct sobriety control it may be necessary to conduct a risk analysis. After the risk has been analyzed, a data protection impact assessment may be needed, depending on the results of the risk analysis. The sobriety check may be conducted by an appropriate person authorized by the employer. In such cases the person must have valid authorization and shall be obliged to obey the data protection rules and keep such data confidential at all times.		

Portugal

Contributors

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

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

Development	Summary	Date	Links
CNPD Directive 2023/1 on TOMs	The Portuguese Data Protection Authority has issued a new Directive regarding the Technical and Organizational Measures (TOMs) that every data controller and processor must consider as a compliance baseline for all data processing activities. The Directive includes guidelines on how to deal with data breaches and lists the TOMs baseline highlighting organizational measures and techniques and, within the scope of the latter, special consideration is given to authentication, infrastructure and systems, email tools, protection against malware, use of equipment in an external environment, storage of paper documents containing personal data and transport of information containing personal data. The Directive may be accessed at https://www.cnpd.pt/comunicacao-publica/noticias/diretriz-sobre-medidas-de-seguranca/ (Portuguese only).	10 January 2023	CNPD Directive 2023/1 (Portuguese only)
CNPD Opinion 2023/22 on the revision of the Government order no. 201-A/2017 regarding the complaints book	Government order no. 201-A/2017, 30 June regards the official format of complaint books that every retail business is obliged to have and keep. This has been revised in order to keep up with current technologic developments. The Portuguese Data Protection Authority has issued Opinion 2023/22 commenting on the possible changes that may arise, and provides recommendations, according to which the tax ID number should be eliminated from the claimant's identification in any complaint, information request, compliment or suggestion forms, since it is not necessary to properly identify data subjects at stake, and therefore violates article 5 of the GDPR.	2 March 2023	CNPD Opinion 2023/22 (Portuguese only)
Draft Law regarding data protection	Portugal has very recently approved a draft Law that is pending publication in the Offical Gazette, to transpose Directive (UE) 2022/211, amending Council Framework Decision 2002/465/JHA	14 March 2023	

Development	Summary	Date	Links
	as regards its alignment with Union rules on the protection of personal data, and Directive (UE) 2022/228, amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data. Both instruments are in the field of criminal law and aim at ensuring alignment of the said instruments amended by the Directives with the EU's rules on the protection of personal data; namely with principles and provisions laid down in Directive (EU) 2016/680 on 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 on the free movement of such data (the Data Protection Law Enforcement Directive).		

Singapore

Contributors

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

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

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

Development	Summary	Date	Links
Korea-Singapore Digital Partnership Agreement & Signing of 3 Memorandums of Understanding	The Korea-Singapore Digital Partnership Agreement ("**KSDPA**") which was signed on 21 November 2022 entered into force on 14 January 2023. The KSDPA's expeditious entry into force is reflective of Singapore and the Republic of Korea's commitment towards integrating both countries' digital ecosystems to unlock new growth opportunities for businesses. Singapore and the Republic of Korea have also signed 3 Memorandums of Understanding ("**MOUs**") to implement the Korea-Singapore Digital Economy Dialogue, facilitate the electronic exchange of data, and enhance cooperation in artificial intelligence. These MOUs are part of ongoing bilateral efforts to develop cooperative projects to implement the KSDPA.	13 January 2023	Press Release Ministry of Trade Press Release of Key Features
First Decision on the Legitimate Interest Exception under the Personal Data Protection Act 2012	The Personal Data Protection Commission ("**PDPC**") recently decided that an e-commerce organisation, Redmart Limited ("**RedMart**"), had met the requirements for reliance on the Legitimate Interests Exception under Paragraph 1, Part 3 of the First Schedule of the Personal Data Protection Act 2012 ("**PDPA**") ("**Legitimate Interests Exception**"). This is the first case under the PDPA that illustrates how the Legitimate Interests Exception may be relied upon by organisations for collecting personal data.	18 January 2023	PDPC's Decision on RedMart

Development	Summary	Date	Links
	The PDPC received a complaint that RedMart had failed to obtain consent and inform its suppliers, who visited RedMart's warehouses to deliver goods and produce sold by RedMart, of the purpose for collecting images of their physical NRICs and other identification documents. In its preliminary decision, the PDPC proposed directions for RedMart to assess its collection of the aforementioned personal data. RedMart proceeded to conduct an internal assessment for its reliance on the Legitimate Interests Exception going forward, and made representations to the PDPC in respect of the preliminary decision. The PDPC subsequently assessed that RedMart had met the requirements for reliance on the Legitimate Interests Exception and had complied with the proposed directions in its preliminary decision. The PDPC found that RedMart has a legitimate interest in deterring acts that could compromise food safety, facilitating investigations into food safety incidents, implementing an enhanced identification system to verify the identities of visitors to a high degree of fidelity, and regulating access to high risk areas. As such, RedMart was found not to be in breach of the PDPA and no direction was issued to RedMart. A key takeaway to note from the PDPC's decision is that in order for an organisation to rely on the Legitimate Interests Exception, it will need to: 1. Conduct and document an assessment determining whether the collection of such data in question is reasonably necessary for the organisation's interests; 2. Identify whether the collection of such data is likely to have an adverse effect on the individuals whose data are being collected; 3. Implement reasonable measures to eliminate, mitigate, or reduce the likelihood of such adverse effects occurring; 4. Determine whether the organisation's interest in such data outweighs the adverse effect on the individuals whose data are being collected (if any) after the above measures are implemented; and		

Development	Summary	Date	Links
	5. Provide reasonable access to information about the organisation's collection of personal data, which can be done by way of disclosure in the organisation's public data protection policy.		
Enhanced measures against scam SMS	All organisations that use alphanumeric Sender IDs must register with the Singapore SMS Sender ID Registry. After 31 January 2023, non-registered SMS Sender IDs are labelled as "Likely-SCAM" to consumers. Organisations which have not registered their Sender IDs are strongly advised to do so.	25 January 2023	Infocomm Media Development Agency's Press Release
Singapore and the European Union Sign Digital Partnership	Singapore and the European Union signed the EU-Singapore Digital Partnership on 1 February 2023 ("**EUSDP**"). The EUSDP is an overarching framework for all areas of bilateral digital cooperation between the EU and Singapore. These areas include issues in the cross-border digital economy such as digital trade facilitation, trusted data flows, electronic payments, and standards and conformance; as well as new and emerging areas such as Artificial Intelligence, digital identities, and 5G/6G. In addition to the bilateral cooperation between EU and Singapore on the aforementioned areas, the EUSDP will also support and enable broader participation in the digital economy through cooperation on digital upskilling for workers, and the digital transformation of businesses as well as public services.	1 February 2023	Press Release
Singapore-European Free Trade Association Digital Economy Agreement	Singapore and the European Free Trade Association ("**EFTA**") launched negotiations on an EFTA-Singapore Digital Economy Agreement ("**DEA**"). The DEA will allow Singapore and EFTA to advance cooperation in the digital domain, including advancing end-to-end trade, enabling trusted data flows, and facilitating a trusted and secure digital environment. In addition to the above, the DEA will also build on and complement ongoing plurilateral efforts including negotiations on the WTO Joint Statement Initiative on E-Commerce.	16 February 2023	Press Release by the Relevant Ministries and Agency of the Singapore Government

Singapore

Development	Summary	Date	Links
Notification to the Monetary Authority of Singapore on Events of Significant Impact (Circular No. ID 03/23)	The Monetary Authority of Singapore ("**MAS**") has set out the revised expectations for licensed insurers regarding the notification to MAS of data breaches: 1. data breaches under the PDPA – MAS should be concurrently notified of data breaches that are required to be notified to the PDPC 2. MAS should be notified of data breaches that meet the criteria under MAS Notice 127 (Notice on Technology Risk Management) and the MAS Guidelines on Outsourcing, based on the timelines indicated within these instruments. 3. other data breaches – MAS should be notified of them on a consolidated basis, within 3 weeks from the last day of each quarter starting from Q1 2023. The breaches to be included should be those identified during the quarter, regardless of whether the breaches had occurred during or prior to the quarter	22 February 2023	MAS Circular No. ID 03/23
Singapore and United States sign a Memorandum of Understanding to Enhance Cooperation Between Both Countries	The Infocomm Media Development Authority ("**IMDA**") of Singapore and the United States Federal Communications Commission ("**FCC**") signed an MOU on 27 February 2023. The MOU seeks to promote bilateral cooperation on telecommunications regulatory policies. The scope of the MOU includes regulatory cooperation and information exchange in emergent areas of communications and connectivity. IMDA and FCC will also be exploring technical cooperation and capacity building in the field of telecommunications.	27 February 2023	Press Release
Cyber Security Agency of Singapore to Launch Scheme to Develop Cybersecurity Health Plans With Funding Support For Small-Medium Enterprises	The Cyber Security Agency of Singapore ("**CSA**") will be launching a scheme to develop cybersecurity health plans with funding support for small-medium enterprises ("**SMEs**"). The scheme is expected to launch in May 2023. The CSA aims to encourage SMEs to improve their cyber defences by going for cyber health "check-ups" and to develop cybersecurity health plans, while working towards national cybersecurity certification such as attaining CSA's Cyber Essentials mark.	28 February 2023	CSA's Press Release Informational Sheet

Development	Summary	Date	Links
	The scheme seeks to alleviate some common challenges SMEs face in implementing cybersecurity measures, such as: 1. lack of in-house cybersecurity staff to address cybersecurity risks; 2. a wide range of cybersecurity solutions and providers in the market, making it challenging for SMEs to prioritise what to implement first; and 3. rising business costs. The CSA will provide funding support to SMEs by co-funding up to 70% of their costs for engaging cybersecurity consultancy services for the first year.		

Slovakia

Contributors

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

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

Development	Summary	Date	Links
Data protection and control plan for 2023	The Office for Personal Data Protection of the Slovak Republic ("**Office**") has published on its website a plan of inspections for 2023 ("**Plan**"). The document consists of the following two parts: **The first part of the Plan and the inspections under it** Within this part, the Office will focus on entities such as the Ministry of Foreign Affairs of the Slovak Republic, the Ministry of the Interior of the Slovak Republic or Europol. An essential criterion is the processing of personal data in information systems operated for the purpose of ensuring the practical implementation of the Schengen and European Union agreements on the territory of the Slovak Republic. A total of 8 inspections are planned. **The second part of the Plan and the controls under it** For the private sector, the second part of the Plan is more pertinent , which relates to inspection of public passenger transport operators, employers and local authorities. Under this part, the Authority intends to focus on the control of compliance with the GDPR and Act No 18/2018 Coll. on the protection of personal data. In addition to verifying, for example, the conditions for consent, the assessment of the impact on data protection, compliance with the principles and lawfulness of processing personal data, the subject of the inspection will also need to verify whether the processing activities carried out reflect the risks associated with specific processing activities or the use of new technologies and procedures (in particular, processes	March 2023	Plan (only in Slovak)

Development	Summary	Date	Links
	capable of significantly affecting the rights and legally protected interests of data subjects). The number of planned inspections in this case is set at 7.		

South Africa

Contributors

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

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

Development	Summary	Date	Links
Call to establish the independence of the Information Regulator	On 8 February 2023, the Information Regulator ("**Regulator**") released a media statement requesting Parliament settle the matter of the independence of the Regulator. The Protection of Personal Information Act, No 4 of 2013 (POPIA), established the Regulator as a statutory body, and requires the Regulator to act independently when exercising its powers and functions. Currently, the Regulator falls under the authority of the Department of Justice and Constitutional Development (DOJ & CD), and relies on the DOJ & CD for funding. The Regulator contends that this is inconsistent with the provisions of POPIA that requires the Regulator to be an independent entity, and could cause a potential conflict of interest as the DOJ & CD is considered a responsible party, and is subject to the POPIA regulations. One of the practical consequences of this untenable situation is that the Regulator can only procure goods and services valued below R1 million directly from suppliers. For all goods and services exceeding this threshold, the Regulator must go through the procurement committees in the DOJ & CD. Giving an example of the inefficacy of this procedure, the Regulator's CEO said there were delays in procuring a management system to assist with the resolution of complaints because it was above the R1 million threshold. The recognition of the Regulator as an independent body would give the Regulator the freedom to fully carry out its mandate in enforcing the provisions of POPIA and resolving queries by data subjects in a timely manner.	8 February 2023	Independence of the Information Regulator-Media Statement

Development	Summary	Date	Links
	Parliament has consequently requested that the National Treasury makes the necessary legislative amendments to Schedule 1 of the Public Finance Management Act, No 1 of 1999, to list the Regulator as a (independent) constitutional body.		
Enforcement of POPIA against the National Department of Health	On 20 February 2023, the Regulator issued a media statement regarding its decision to refer the National Department of Health ("**NDoH**") to the Enforcement Committee ("**Committee**"). This decision comes after several requests for information from the Regulator to the NDoH regarding the management of personal information collected by the NDoH during the COVID-19 pandemic were ignored. An enforcement notice issued by the Committee has the same effect as a court order. The Regulator, in its mandate to enforce and monitor compliance with POPIA, sought confirmation and guarantees from the NDoH that the personal information, collected during the management of the COVID-19 pandemic, had been de-identified or destroyed within six weeks after the national state of disaster had been lifted. The Regulator repeatedly requested the NDoH to provide the requested confirmation and guarantees, as well as a report from an expert third party IT security expert regarding the reliability and suitability of the NDoH's IT security safeguards. However, no such response was received. Ultimately, the Regulator referred the matter to the Committee, in accordance withsection 92(1) of POPIA. It appears that the NDoH might be the first responsible party fined by the Regulator since its establishment in August 2022. This comes after several complaints that the Regulator is too lenient in holding transgressors accountable in law, considering that South African organisations faced a number of data breaches since POPIA came into operation in July 2021. If the Regulator, and the Committee, go through with this action against the NDoH, and fines the NDoH, it may restore the confidence of the public in the role of the Regulator, and in entrusting their personal information with public and private bodies, as well as ensuring compliance by the Regulator by these entities with the requirements under POPIA.	20 February 2023	POPIA Enforcement - Information Regulator Media Statement

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
Swedish DPA criticizes the police's e-mail management	The Swedish DPA criticized the police for their management of e-mails that contained information about suspects and victims. Employees had sent sensitive e-mails to unauthorized recipients due to accidently misspelling their internal e-mail domain when the recipient's e-mail address was entered. According to the police, an individual or group outside the organisation has registered internet domains with similar spellings to the one used by the police and thus obtained e-mails that were intended for internal matters.	17 January 2023	Press statement (in Swedish) Decision (in Swedish)
Swedish DPA issues an administrative fine against a county for sending letters by mail where sensitive personal data was visible in the window envelope	The Swedish DPA issued an administrative fine of SEK 200,000 against a county which had sent appointment letters by regular mail to patients where sensitive personal data was visible in the window envelopes. The Swedish DPA concluded that the processing of personal data was partially automated when the appointment letters were printed and that GDPR was therefore applicable. The main issue was that on the window envelopes of the appointment letters, the care facility was clearly visible. As a result, sensitive personal data of patients were disclosed without authorization to an unknown number of people who came into contact with the letters. The incident concerned over 2,500 letters that were sent per year, including to a treatment centre and a therapy clinic for children and young people.	18 January 2023	Press statement (in English) Decision (in Swedish)
Swedish DPA issues a reprimand against an insurance company for	The Swedish DPA has received a complaint that an insurance company sent sensitive personal data by e-mail without sufficient data protection. An audit was initiated to investigate whether the	23 January 2023	Press statement (in Swedish) Decision (in Swedish)

Development	Summary	Date	Links
sending sensitive personal data by e-mail without adequate security	insurance company had ensured an appropriate level of security to protect the personal data being processed. In the decision, the Swedish DPA states that the insurance company had sent the e-mail to the complainant with encryption, but that the e-mail was only encrypted during the transmission from the company's e-mail server to the e-mail server provided by the complainant's operator. The above meant that the encryption ended before the e-mail had reached the final recipient. Consequently, there was a risk that unauthorized persons could read the e-mail in plain text after the encrypted transmission had ended. In response, the insurance company now requires that customers log into their account by using an advanced electronic signature in order to read e-mails sent by the company.		
Swedish data protection officers point to problems applying GDPR	The Swedish DPA has now published the report 'Data protection in practice', which is based on a survey of Swedish data protection officers ("**DPO**") in over 800 organisations. The report provides an indication of the conditions under which data protection is applied in organisations required to have DPOs. According to the report, less than half of the responding DPOs assess that their own organisation works systematically with data protection. Furthermore, only half of the DPOs feel that they are able to explain the importance of data protection issues to management.	27 January 2023	Press statement (in English) Survey report (in English)
Swedish DPA will focus on initiating more audits based on complaints from data subjects	The Swedish DPA notes in their annual report for 2022 that, amongst other things, one of their top priorities will be to initiate more audits based on complaints from data subjects. Most audits have historically been initiated based on specific focus areas such as processing large amounts of sensitive personal data or the use of CCTV. Other figures from the annual report of 2022 include the following:	22 February 2023	Press statement (in Swedish) Annual report (in Swedish)

Development	Summary	Date	Links
	1. the number of submitted complaints from data subjects have decreased from 2,847 to 2,245, approximately 21% decrease compared to last year 2. audits initiated regarding CCTV have almost doubled compared to last year, from 22 to 42 cases. The number of completed audits have increased significantly compared to last year, from 6 to 38 cases. The absolute majority, approximately 90% of the audits for 2022, have only resulted in reprimands (i.e. a warning) or an order (i.e. taking a specific action, not ban on processing) 3. the number of reported personal data breaches have decreased from 5,767 to 5,333 compared to last year, approximately an 8% decrease 4. the number of BCR applications have decreased from 89 to 39, approximately 57% decrease compared to the year prior. The time for the Swedish DPA to handle BCR cases has increased significantly compared to last year, from 44 to 146 days 5. the number of new Data Protection Officer registrations with the Swedish DPA remains steady at 2,121 registrations, compared to last year which had 2,021 registrations 6. only five cases in 2022 have resulted in the Swedish DPA issuing an administrative fine. The total amount of administrative fines issued for the year was SEK 9,720,000. The single largest fine was against a bank that lead to an administrative fine of SEK 7,500,000		
Swedish DPA initiates audit on a county regarding e-mail management and sensitive personal data	The Swedish DPA has received complaints that a county is using Microsoft Outlook to send and store health data relating to patients. As a result, an audit was initiated to find out whether the county has sufficiently taken into account the patients' right to privacy when using Microsoft Outlook. No audit statement has been published but based on the press statement it is likely that the Swedish DPA will investigate whether the county has performed a data protection impact assessment and possibly a transfer impact assessment with	23 February 2023	Press statement (in Swedish)

Development	Summary	Date	Links
	regard to the direct or indirect transfer of personal data to the U.S. via the use of Microsoft Outlook. The outcome of this matter may provide valuable insight into whether the Swedish DPA, in principle, accepts the use of a U.S. e-mail client or exchange for storage or transmission of personal data.		
Swedish DPA criticizes a debt collection agency for lack of routines to manage misleading advertisement	The audit against a debt collection agency for sending out misleading advertisements has now been completed. The decision to audit the company was previously reported in Updata Edition 14. The Swedish DPA concludes that the debt collection agency lacks sufficient routines to ensure that client companies have a lawful basis to send out advertisement to individuals. The issue at hand was that the debt collection agency had, on behalf of these client companies, sent advertisements to individuals that was considered misleading as the marketing material had the appearance of an invoice. No administrative fine was issued, however, the Swedish DPA ordered the debt collection agency to implement routines that prevent similar incidents from occurring.	7 March 2023	Press statement (in Swedish) Decision (in Swedish)
Swedish DPA provide further clarity on legitimate interest to use CCTV in a decision against a pharmacy company	The Swedish DPA has completed an audit against a pharmacy company regarding the company's use of CCTV inside their logistic centre. The Swedish DPA concluded in their decision that the company had a legitimate interest to use CCTV for the purpose of crime prevention, to deal with technical problems in the production of medicinal goods and to check how much of their delivery area was available for future deliveries. It was explicitly confirmed by the Swedish DPA that purely economic interests for using CCTV can be sufficient to establish a legitimate interest. Regarding the use of CCTV for crime prevention, the Swedish DPA further clarified that such purpose does not necessarily require that incidents have occurred in the past. In this case it was sufficient to state that medicinal goods are generally considered more theft-prone.	16 March 2023	Press statement (in Swedish) Decision (in Swedish)

Sweden

Development	Summary	Date	Links
The Swedish Supreme Court orders the Court of Appeal to try whether Sweden's constitution exempt companies from being subject to GDPR when maintaining databases of criminal cases	A Swedish company maintains a publicly available database of criminal cases from Swedish courts. A data subject sued the company for publishing information on their website that the data subject had been criminally charged in several cases. In the lawsuit, the data subject also requested the deletion of their personal data pursuant to article 17 GDPR ('right to be forgotten'). The District Court dismissed the claim and the Court of Appeal did not grant a leave to appeal, citing that the company had been issued a so-called "publication certificate" in accordance with the Fundamental Law on Freedom of Expression. The company's database was therefore not subject to the GDPR pursuant to the protection enshrined under the Swedish constitution. The Supreme Court notes that the case raises a question about the relationship between GDPR and the constitutional protection under Swedish law concerning information about prosecutions on websites. As there are no guiding rulings on the matter, the Supreme Court considers it important that the case is tried by the Court of Appeal.	21 March 2023	Link

Switzerland

Contributors

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

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

Oliver Scharp
Associate
T: +41 58 255 5650
oliver.scharp@
eversheds-sutherland.ch

Development	Summary	Date	Links
The National Council is in favour of obliging operators of critical infrastructures in future to report cyber attacks with major damage potential to the National Cyber Security Centre (NCSC) within 24 hours	Through a corresponding amendment to the Information Security Act, operators of critical infrastructures will have to report cyber attacks to the National Cyber Security Centre ("**NCSC**"). The Federal Council and Parliament, the Office of the Attorney General of Switzerland, the Armed Forces, universities, banks, private insurance companies and financial market infrastructures, healthcare facilities, medical laboratories, social insurance companies, the SRG, postal service providers, data centre providers, etc. would be subject to the reporting obligation. In the dispatch and the draft, the deadline of 24 hours between the incident and the report as well as the fine for a breach of the reporting obligation despite the NCSC's order were controversial in the National Council. The majority in the National Council left it at the Federal Council's draft in both cases. The bill now goes to the Council of States, which will deal with it in the summer session.	16 March 2023	
The FDPIC announced on 27 January 2023 that it was revising its website and launching a new reporting portal by 1 September 2023	In connection with the revision of the Swiss Data Protection Act, the FDPIC draws attention to the new reporting portals which he intends to make available when it comes into force:	27 January 2023	

Development	Summary	Date	Links
	1. notification of processing directories (only federal bodies; Art. 12 para. 4 FADP) 2. notification of data protection advisors (federal bodies only; Art. 27 para. 2 FADP) 3. notification of high-risk data breaches (Art. 24 nDSG; Art. 15 FADP) In addition, the FDPIC's website will be revised, with information in line with the revised law and with explanations of new instruments such as the data protection impact assessment. In contrast to notification under the GDPR, notification obligations under the Swiss Data Protection Act are not subject to any specific deadline. They must be reported as soon as possible.		

United Kingdom

Contributors

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

Carolyn Sullivan
Associate
T: +44 20 7919 0941
carolynsullivan@
eversheds-sutherland.com

Development	Summary	Date	Links
Regulation of communication service providers by the ICO	On 20 January 2023, the Information Commissioner's Office ("**ICO**") made a statement on the obligations of public electronic communications service providers ("**CSPs**"). This was done under Regulation 5A of the Privacy and Electronic Communications Regulations 2003 ("**PECR**"). In brief, the ICO had said it was going to relax the reporting requirements for CSPs as this was too onerous and was creating a disproportionate volume of reports, when considered alongside the likely resulting risk. However, shortly after, this statement was taken down and reviewed as a result of a desire to offer more transparency in regard to CSPs. The ICO has a three-year strategic plan, known as the ICO25, which aims to lessen the burden and costs of requirements to comply with data protection. In accordance with Regulation 5A PECR, CSPs must notify the ICO within 24 hours of finding out about a personal data breach. If this is not complied with, the CSP can receive a penalty of £1,000 from the ICO. Essentially, this requirement to notify the ICO is in place of the reporting obligations required by UK GDPR.	20 January 2023	ICO Statement
ICO decision provides guidance on Facial Recognition Technology in schools	The question of how to validly identify and secure transactions within schools has been a challenge for some time. In a recent decision, the Information Commissioners Office ("**ICO**") has published a letter explaining its views on the use of Facial Recognition Technology (FRT) in schools. Whilst the ICO has not discouraged schools from embracing new technology, it has set out clear guidance to follow regarding the data protection considerations and compliance which must be considered alongside the use of such technologies. Recognising that, particular challenges exist in the following areas:	31 January 2023	Letter

Development	Summary	Date	Links
	1. ensuring a valid lawful reason for processing: given the processing of biometric data, this will most often be consent, but this must be obtained from the parent (if under 12) and from the child (if 12 or over) and must be explicit to meet data protection standards; 2. ensuring fairness and transparency: privacy notices must be fully informed and must be written using "age appropriate language", in an "intelligible and easily accessible form". This is often easier said than done in practice; and 3. data minimisation: the processing undertaken needs to be limited to what is necessary to achieve those identified lawful processing purposes. This needs to be assessed and recorded to help shield against future complaints and claims It is hard not to see the wider guidance here as a homage to our old friend, the Data Protection Impact Assessment (**"DPIA"**). Done properly, a DPIA would ensure a proper assessment of lawful basis, fairness, transparency and data minimisation as a single source of truth. Whilst certainly not universally viewed with great warmth in the sector, this is another reminder that early detailed thinking and a clear, contemporaneous audit trail are the most powerful shields to have in this area to regulatory enquiry, enforcement and complaint. Viewed another way, you could read this guidance as making it pretty clear that if you have such systems in place (or indeed are undertaking high risk processing in other areas) without a good DPIA, you are very much leaving yourself open to challenge if complaints are received.		
Privacy by design to become an ISO standard	The International Organisation for Standardisation ("**ISO**") is expected to adopt "Privacy by Design" as an ISO standard. "Privacy by Design" is an approach where organisations consider and seek to address data protection issues at the design phase of any system, product or service, as well as throughout the lifecycle of that system, product or service. The phrase and concept initially came about in 2009 as a set of principles, and have subsequently been incorporated into the GDPR as a legal requirement. Its adoption as an ISO standard will provide organisations with a way to demonstrate their compliance with	January 2023	ISO 31700

Development	Summary	Date	Links
	the privacy by design obligations in relation to systems, products and services. Known as ISO 31700, the standard will have 30 requirements, including: 1. how to enable consumers to exercise their rights under data protection law; 2. designing and documenting privacy controls and security measures; and 3. identifying, preparing for and managing data breaches and conducting risk assessments.		
UK's landmark data adequacy decision with South Korea comes into effect	The UK's data adequacy decision with South Korea has come into effect. The decision will allow UK personal data to be transferred to South Korea without the requirement of conducting a transfer impact assessment or entering into additional safeguards, such as the UK's international data transfer agreement or binding corporate rules. The UK and South Korea had agreed to a data adequacy agreement in principle in July 2022, which was followed by an announcement in November 2022 that the Government was satisfied that an adequacy decision would be suitable. On 19 December 2022, this was formalised and brought into effect via the Data Protection (Adequacy) (Republic of Korea) Regulations 2022. This decision is notable for being the first UK-created adequacy decision published following the UK's departure from the EU. The decision is expected to strengthen the relationship between the UK and South Korea, increase research and innovation and bring financial gains to both sides.	January 2023	The Data Protection (Adequacy) (Republic of Korea) Regulations 2022 (legislation.gov.uk)
UK and USA agree data bridge deliverable	Following on from the announcement in October that the UK Government was working on reaching an adequacy decision with the USA, senior representatives from both the UK and US governments have met in Washington D.C. to discuss technology and data cooperation. The two countries discussed key deliverables to address in 2023, which include an attempt to "finalise and implement a data bridge for US-UK data flows". Representatives from the two countries agreed to review progress on a quarterly basis, with the next formal meeting in January 2024.	January 2023	UK-US Joint Statement: New Comprehensive Dialogue on Technology and Data and Progress on Data Adequacy

Development	Summary	Date	Links
Government consulting on draft legislation to support identity verification	The UK Government is currently consulting on draft legislation to support identity verification. The draft legislation, the Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023, aims to make identity verification online easier and more reliable. The draft legislation will provide the Government with a legal basis to share personal data for identity verification purposes across various governmental departments and public bodies. In addition, it will create a new verification system on the www.gov.uk website, which will allow users to verify their identity just once to be able to access numerous Government services online. Responses to the consultation are open until 1 March 2023.	January 2023	Consultation on draft legislation to support identity verification
ICO makes changes to publicly available information	The ICO has made changes to what information it publishes about the work, investigations and actions it has been involved in. The two big developments in this regard are that the ICO has started publishing details of: 1. the reprimands it has given. These are formal decisions made by the ICO that an organisation has infringed data privacy law. Publication of this information has been backdated to January 2022. Previously, the ICO only published details of its more stringent actions, eg fines it had levied and enforcement notices 2. data protection complaints (whether they are upheld or not); actual or potential data breaches which have been self-reported by controllers (dealt with by the ICO's personal data breach team, but not referred to the ICO's investigations department for possible regulatory action); civil investigations (including "incidents" which were not progressed to a full investigation); and cyber investigations, each published in Excel spreadsheets going back to Q4 2020/2021 While these developments are in line with the UK ICO's push toward transparency, and the publishing of reprimands was forewarned in a November 2022 speech by John Edwards (the UK's Information Commissioner), they were introduced quietly at	January 2023	How the ICO enforces: a new strategic approach to regulatory action

Development	Summary	Date	Links
	the end of 2022 which may have caught some organisations off-guard.		
ICO publishes report on emerging technologies	On 15 December 2022, the ICO published its first 'Tech Horizons Report'. This report is the first of a new series to be released annually by the ICO, and sets out views on emerging technologies. In the report, the ICO set out four common challenges it sees that may harm privacy and trust in emerging technologies: 1. these technologies are collecting personal information in ways that may not be "transparent" to people and over which they may not have "meaningful control" 2. the technologies' complex data ecosystems make it difficult for people to understand how their data is being processed 3. some technologies are collecting more personal data than they may need to 4. many technologies are collecting sensitive personal data, such as biometric or health data, that may require additional safeguards The report focuses on four technologies expected to have a "novel and significant implication for privacy over the next two to five years", being: 1. "consumer health-tech" – wearable devices that help people assess their health 2. "internet of things" – objects that connect and share information with the ability to interact with the external environment 3. "immersive technology" – augmented and virtual reality hardware 4. "decentralised finance" – software that employs blockchain to support peer-to-peer financial transactions	January 2023	Tech Horizons Report
High Court case clarifies the use of personal data in litigation proceedings	The High Court case of Dixon v North Bristol NHS Trust has provided insight into the interplay between UK GDPR and litigation proceedings. The case concerned a Claimant's request	January 2023	Decision

Development	Summary	Date	Links
	for an interim injunction to prevent the disclosure of a number of documents. This application was part of a wider litigation proceeding. Amongst other reasons, the Claimant alleged that it would be a breach of the Claimant's data protection rights under the UK GDPR for the documents to be disclosed. The Defendants had argued that the disclosure would be lawful pursuant to: 1. UK GDPR Article 6(1)(c) (the 'processing must be necessary for compliance with a legal obligation to which the controller is subject') and/or 2. UK GDPR Article 6(1)(e) ('processing is necessary for the performance of a task carried out in the public interest') The Claimant argued that processing in accordance with Article 6(1)(c) UK GDPR should be interpreted narrowly. The Judge found this to be incorrect, stating Article 6(1)(c) does not give a data subject a "veto" on what data can be disclosed, and consent is a separate, and only one of, the lawful bases under which personal data can be processed under UK GDPR. The Judge therefore stated that the Defendants would likely succeed in being able to disclose their documents under UK data protection law, specifically: 1. UK GDPR Article 6(1)(c) and/or 6(1)(e) 2. if the latter, in conjunction with Section 8 of the Data Protection Act 2018 (which expands on Article 6(1)(e) UK GDPR) This case indicates that UK GDPR will not prevent personal data being used in litigation proceedings where this disclosure is necessary. On the contrary, the UK GDPR has specific provisions that allow for disclosures for legal proceedings which enable the lawful use of personal data during litigation proceedings where it is necessary.		
New FOI resources to support public authorities	As part of their ICO25 plan commitments, the Information Commissioner's Office ("**ICO**"), has announced a number of new initiatives and support systems that they have introduced to	February 2023	ICO25 Plan FOI resources

Development	Summary	Date	Links
	improve their Freedom of Information services available for public authorities. A new 'Upstream Regulation team' has been set up with the aim of promoting "good practice", a specific duty listed within the Freedom of Information Act 2000 ("**FOIA**"). To achieve this aim, the team have been working to examine what public authorities need help with and how the team can support. Independent research has been conducted and a survey has been undertaken with responses gathered from public bodies. Internally, input has also been gathered from the ICO's casework and stakeholder engagements. The ICO have also released a suite of documents to assist public bodies in complying with FOI requests and meeting the response timescales. These resources include an FOI self-assessment toolkit allowing you to "assess your current FOI performance" and consider where improvements can be made. A link to the resources can be found here. Additionally, Practice Recommendations have also been issued and can be viewed on the ICO's website here. Practice Recommendations set out the ICO's view on whether public authorities have complied with their obligations under FOIA, and often set out the steps that should have been taken for the authority to conform. These recommendations therefore provide good steps and examples for public bodies to follow when ensuring they are acting in compliance with the Act. Finally, the ICO also encourage publication of information that is safe to disclose and that is in the public interest and they have released a publication scheme report. This report includes "recommendations to help support public bodies comply with this area". This additional support and guidance materials from the ICO is welcomed and will assist public bodies to ensure they are complying with their responsibilities under FOIA.		Publication scheme report
ICO guidance	The ICO has published: 1. guidance on privacy in the product design lifecycle: this is aimed at technology professionals with responsibility for apps, websites or other tech products that collect, manage or share personal data, to help them embed data protection into their products and services. The guidance looks at key privacy considerations for each stage of product design	March 2023	Guidance on privacy in the product design lifecycle AI guidance

Development	Summary	Date	Links
	lifecycle, from kick-off to post-launch, and includes examples of good practice and steps for organisations to take when designing websites, apps and technology, products and services to help them understand what organisations must, should and could do to comply; and 2. updated guidance on AI and data protection: updates focus on the requirements for fairness in AI, explaining in the context of using AI to process personal data, how to ensure compliance with the transparency principle, what to cover in a data privacy impact assessment, how to ensure fairness and how to ensure lawfulness.		
Information Tribunal rules on Experian appeal against ICO action	The First-Tier Tribunal has given judgment on the appeal by Experian Limited ("**Experian**") against an ICO enforcement notice which required Experian to take steps to change how it processes personal data for direct marketing purposes. While the Tribunal agreed with the ICO that Experian had not acted lawfully in failing to provide a group of over 5 million individuals with a privacy notice, it rejected a number of the ICO's findings, including that Experian's privacy notice was not transparent, that using credit reference data for direct marketing purposes was unfair, or that Experian did not properly assess its lawful basis. The judgment provided a Substitute Decision Notice, the requirements of which are significantly less arduous than those under the ICO's original Enforcement Notice and include an obligation on Experian to provide privacy notices to previously affected data subjects The ICO has announced that it plans to appeal the Tribunal's decision.	March 2023	Decision
Reform of UK data protection law in the pipeline	The Data Protection and Digital Information (No. 2) Bill has been introduced to Parliament by the Government. This replaces the previous version of the Bill that was introduced last summer and which has now been withdrawn. The purpose of the Bill is to update and simplify the UK data protection framework in order to reduce compliance burdens for businesses, whilst ensuring that the UK's high data protection standards are retained. The Government has publicised the Bill as a "common sense led" UK version of GDPR which will "cut down pointless paperwork for businesses and reduce annoying cookie pop-ups". The reforms will impact all UK businesses. Headline reforms include:	March 2023	Bill

Development	Summary	Date	Links
	1. organisations will only need to keep records of personal data processing if their processing activities are likely to pose high risks to the rights and freedoms of data subjects; 2. creation of a new lawful basis for the processing of personal data where such processing is necessary for a recognised legitimate interest set out in secondary legislation; 3. addition of non-exhaustive examples of the types of processing that may be necessary for a legitimate interest of the controller, including direct marketing, intra-group transmission that is necessary for internal administrative purposes and processing that is necessary to ensure the security of network and information systems; 4. improved clarity on when safeguards for solely automated decision-making apply; 5. broadening the circumstances in which organisations can refuse to answer a data subject access request, so that requests can be refused where they are vexatious or excessive; 6. clarifying rules on international transfers of personal data, with a focus on data protection outcomes; 7. making it easier to use personal data for scientific research; 8. increasing fines for nuisance marketing; 9. creating a framework for the regulation of UK digital verification services; 10. facilitating creation and operation of smart data schemes; and 11. reform of the Information Commissioner's Office. We will be monitoring the Bill's progress, so watch out for future updates.		

United States

Contributors

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

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

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

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

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

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

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

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

Mary Park
Konexo Attorney
T: +1 714 864 4236
marypark@
konexoglobal.us

Development	Summary	Date	Links
The California Privacy Rights Act Takes Effect, Extending Privacy Protections	On January 1, 2023, the California Privacy Rights Act ("**CPRA**") took effect, significantly amending the California Consumer Privacy Act ("**CCPA**"). Some key provisions of the CPRA include: 1. changes to/or addition of definitions of "sensitive" personal information, "third party", and "profiling"; 2. changes to business obligations: i. limits data retention and requires disclosure of retention periods; ii. adds a right to limit the use and disclosure of sensitive personal information; iii. adds a right to correct inaccurate personal information; iv. extends consumer's opt-out rights to the sharing of personal information for cross-contextual advertising; v. extends the non-discrimination provision to include non-retaliation; vi. adds contract requirements for all persons that receive personal information; 3. increased rights of children; 4. establishment of the new California Privacy Protection Agency (CPPA); 5. new rulemaking requirements on insurance and cybersecurity and privacy; and 6. extension of the scope of the private right of action. Enforcement of the CPRA will not begin until July 1, 2023, and enforcement will apply only to violations occurring on or after that date. However, it should be noted that the CCPA's provisions remain in effect and enforceable until that date.	1 January 2023	CPRA CCPA

The Virginia Consumer Data Protection Act Takes Effect in Virginia Providing a Comprehensive Consumer Privacy Legislation	On January 1, 2023, the Virginia Consumer Data Protection Act ("**VCDPA**") went into effect. Like the CCPA, the VCDPA provides a comprehensive consumer privacy legislation by providing consumers with certain rights related to their personal data, and can apply to businesses which are not headquartered or incorporated in Virginia, but which nonetheless do business there. The VCDPA will be enforced by the Virginia Attorney General and allows for a 30-day cure period, but uncured non-compliance can result in a civil penalty of up to $7,500 per violation. Unlike the CCPA, the Act does not create a private right of action for citizens, and it does not apply in the employment or B2B contexts.	1 January 2023	Virgin Consumer Data Protection Act
The Student Test Taker Privacy Protection Act Takes Effect in California to Protect Information about Students Taking Proctored Tests	On January 1, 2023, the Student Test Taker Privacy Protection Act ("**Act**") took effect in California. The Act limits businesses that provide proctoring services in educational settings to collect, use, retain, and disclose only the personal information strictly necessary to provide those services. However, the Act does not prohibit a business from collecting, using, retaining, or disclosing personal information if doing so is necessary to comply with federal, state or local law or agency.	1 January 2023	The Student Test Taker Privacy Protection Act
Assembly Bill 2089 Takes Effect To Further Expand **Medical Privacy to Additional Types of Information**	On January 1, 2023, Assembly Bill 2089 took effect in California. Assembly Bill 2089 amends California's Confidentiality of Medical Information Act ("**CMIA**"), which prohibits certain businesses from using medical information for any purpose that is not necessary to the provision of health care services, by expanding its definition of medical information. The revised definition includes mental health application information, which generally is defined as information related to a consumer's mental health or substance use disorder collected by a mental health digital service. Further, the law adds businesses that offer certain mental health digital services to within the purview of the CMIA.	1 January 2023	Assembly Bill 2089
Senate Bill 1228 Takes Effect In California To Prevent Misuse Of	On January 1, 2023, Senate Bill 1228 took effect in California. Senate Bill 1228 creates procedures for known reference samples of DNA from a victim of a crime or alleged crime, from	1 January 2023	Senate Bill 1228

DNA Information By Law Enforcement	any individual that voluntarily provided DNA for the purpose of exclusion, as well as for any profiles developed from the samples. These procedures, among other things, require law enforcement to use these DNA samples only for purposes directly related to the incident being investigated, prohibit law enforcement from comparing these DNA samples to other samples that are unrelated to the incident being investigated, and prohibit law enforcement from including these DNA profiles in databases that allow comparison or matching with profiles derived from DNA from crime scenes.		
Assembly Bill 984 Takes Effect In California to Prohibit the Use of Tracking Devices in Certain Types of New Alternatives to Vehicle License Plates	On January 1, 2023, Assembly Bill 984 ("**Bill**") took effect in California. Assembly Bill 984 requires the Department of Motor Vehicles to establish a program authorizing an entity to issue alternatives to existing vehicle identification systems such as stickers, tabs, license plates and registration cards. These alternatives could include, for example, electronic devices such as digital license plates. Generally, the law prohibits these alternatives from being equipped with GPS or location tracking technologies when used on private vehicles. However, the Bill allows such technology to be incorporated into these alternative devices for fleet and commercial vehicles, but imposes certain restrictions and notification requirements on the use of such technology. Specifically, while the law generally prohibits employers from using alternative devices with tracking technology to monitor employees, it does allow employers to use such devices to surveil employees during work hours if such surveillance is strictly necessary to an employee's performance of duties. Under the law, employers must first notify employees that they will be monitored and allow them to deactivate the device's monitoring capabilities outside of work hours. Notice to employees must include specific information such as what activities will be monitored, what employee data will be collected and where data will be stored.	1 January 2023	Assembly Bill 984
Texas District Court Approves $11 Million Settlement to Resolve Data Breach Class Action	On January 4, 2023, the U.S. District Court for the Northern District of Texas approved an $11 million settlement resolving claims against insurance technology provider Zywave Inc. (Zywave) and its subsidiary Insurance Technology Corp (ITC) stemming from a data breach that allegedly exposed personal	4 January 2023	Decision

	information of over 4 million individuals. The district court concluded the settlement was "fair, reasonable, and adequate, and in the best interest of the Settlement Class," certifying that the prerequisites under Rule 23 of the Federal Rules of Civil Procedure had been met.		
FCC Proposes Changes to Customer Data Breach Reporting Requirements	On January 6, 2023, the Federal Communications Commission ("**FCC**") released a Notice of Proposed Rulemaking to change the data breach reporting requirements for customer proprietary network information ("**CPNI**") that apply to US telecommunications carriers. The FCC seeks to align the requirements with the Cybersecurity and Infrastructure Security Agency's new incident reporting system. The key changes include the following: 1. an expansion of the definition of "breach" to include inadvertent access, use or disclosures of customer information; 2. requiring carriers to notify the FCC of any data breaches as soon as practicably possible; 3. requiring carriers to notify customers of CPNI breaches "without unreasonable delay" after discovery of a breach and notification to law enforcement, unless a law enforcement agency requests a delay; and 4. implementing equivalent measures to telephone and video relay service providers.	6 January 2023	Notice of Proposed Rulemaking
New NIST AI Framework Offers Guidance on Risk Management and Governance for Trustworthy AI Systems	On January 26, 2023, the National Institute of Standards and Technology (NIST) released its AI Risk Management Framework ("**AI RMF**" or "**Framework**"). The AI RMF is a resource for organizations designing, developing, deploying, or using artificial intelligence (AI) systems to help manage the risks of AI and promote trustworthy and responsible development and use of AI systems. The Framework is voluntary and flexible – meaning organizations of all sizes and across all sectors can adapt it to their specific use cases.	26 January 2023	AI Risk Management Framework

California Attorney General Conducts CCPA Investigative Sweep	On January 27, 2023, in observance of Data Privacy Day, California Attorney General Rob Bonta sent letters to various businesses alleging CCPA violations – this time, focusing on companies with mobile applications in the retail, travel and food services industries.	27 January 2023	Press Release from the California Attorney General Office
Increased compliance with AI	With the growing presence of AI-based decision making in the EU and the United States, data privacy laws are being implemented to protect employees' personal data used by businesses through automated decision-making processes. This includes increased transparency on the use of individuals' data and consent options. By way of example, New York's Local Law 144 will regulate how organisations use automated employment decisions tools, in contrast with the Consumer Privacy Act in California (the CCPA), recently amended by the California Privacy Rights Act (the CPRA), which expands data privacy law. This will offer protection to job applicants and employees, in addition to dealings between businesses and independent contractors. Businesses will need to make certain they are compliant with AI and data privacy regulations in the future.	February 2023	New York Local Law
New York City Delays Enforcement of its Artificial Intelligence Bias Audit in Employment Law as Rule-Making Continues	New York City (NYC) has delayed to April 15, 2023 the enforcement of its first law on bias in artificial intelligence (AI) tools used in employment. Local Law 144 of 2021 prohibits employers in NYC from using artificial intelligence (specifically referred to as "automated employment decision tools," or AEDTs) to screen candidates for hiring or promotion unless the employers first conduct an audit to determine whether there is bias present in the tool. The law was originally intended to go into effect on January 1, 2023, but enforcement has been delayed until April 15, 2023 as rule-making around the law continues.	February 2023	Local Law 144 of 2021
FTC Diagnoses Common Digital Practices as Both UDAP and Breach	On February 1, 2023, the Federal Trade Commission ("**FTC**") announced it was diagnosing GoodRx's use of tracking pixel codes and analytics, its digital strategy, as not only an unfair or deceptive act or abusive practice but also as a data breach. Reaching well beyond the healthcare space, the FTC, state regulators, and courts can be expected to grapple with whether	1 February 2023	FTC Press Release Eversheds Article on FTC diagnoses

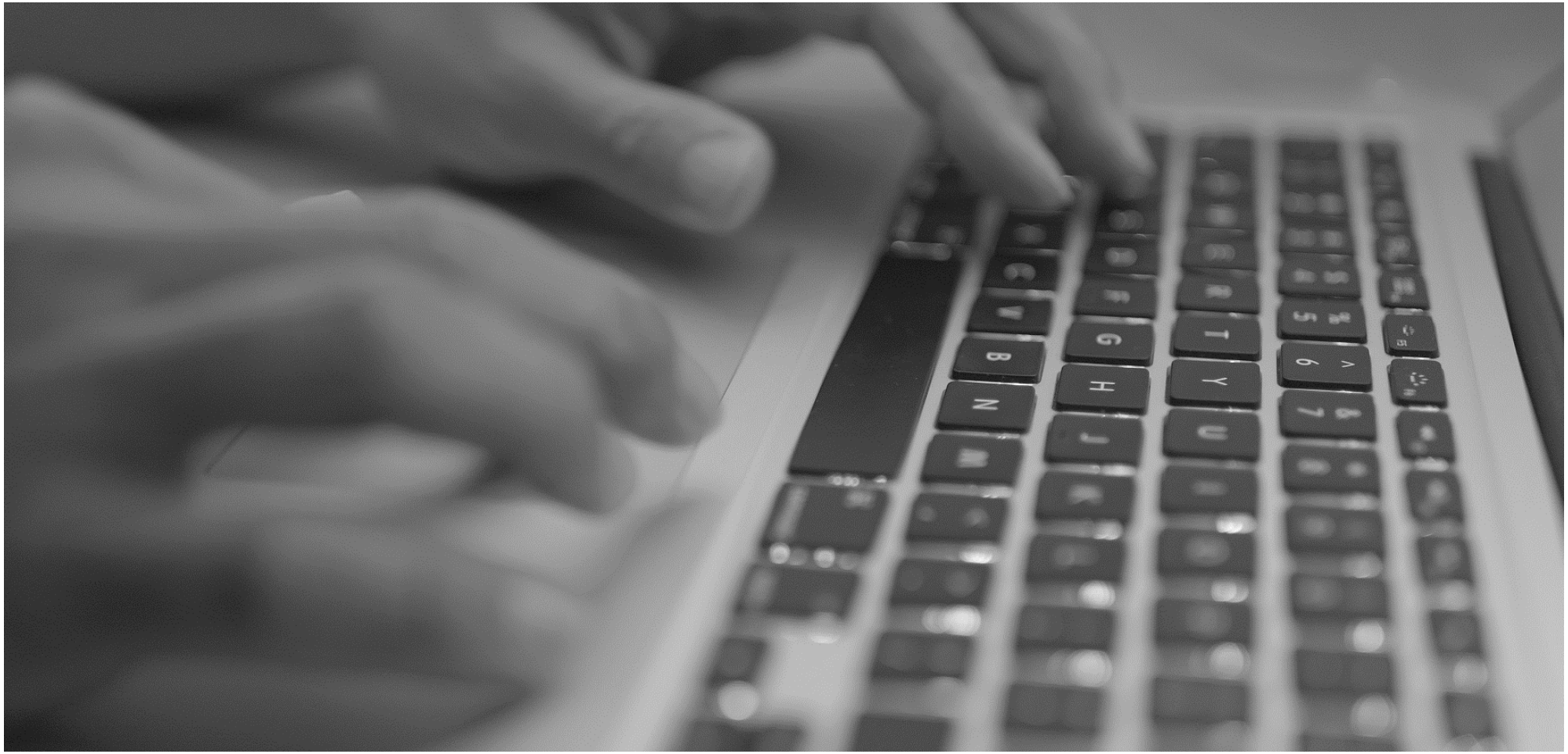
	or not companies' digital strategies (such as tracking codes and related analytics including those that target information presented to consumers) run afoul of the privacy promises they make to consumers.		
NAIC Proposes New California-Style Privacy Model Law for Insurance	On February 1, 2023, the NAIC Privacy Protections Working Group released a draft of a new model law for comment, the Insurance Consumer Privacy Protection Model Law (#674), which proposes to substantially limit the ability of insurance licensees to use consumer personal information and expand the privacy rights and protections provided to insurance consumers. These use limitations and rights provisions are similar to, and in some cases considerably more stringent than, those within the California Consumer Privacy Act (CCPA) and the UK/EU GDPR.	1 February 2023	Insurance Consumer Privacy Protection Model Law
Colorado Division of Insurance's First Installment of Regulations Prohibiting the Use of External Consumer Data and Algorithms	On February 7, 2023, the Colorado Division of Insurance released a draft of the first of several regulations to implement S.B. 21-169, Colorado's 2021 law prohibiting insurers from using external consumer data and information sources ("**ECDIS**") that unfairly discriminate against specified protected classes. The proposal covers governance and risk management framework requirements for life insurers and will be followed soon by a separate proposal covering testing. The proposed regulation makes clear that insurers will be held accountable, at the board level, for all aspects of their use of ECDIS, algorithms and predictive models.	7 February 2023	Draft of Proposed Governance Regulation
Two Illinois Supreme Court Decisions Expand Scope of Potential Damages Under Biometric Information Privacy Act	For several years, companies that collect, use, and store the biometric information of Illinois residents have lived in fear of violating the Biometric Information Privacy Act ("**BIPA**"), due to a tidal wave of class action filings resulting in multi-million dollar settlements and verdicts in Illinois and elsewhere. In the wake of back-to-back opinions issued by the Illinois Supreme Court in February 2023, companies subject to BIPA now face even greater legal exposure. The decisions, which establish a five-year statute of limitations period, and allow for accrual of each independent use of biometric information, respectively, create the potential for astronomical statutory damages awards that will put businesses at risk of financial peril. Additionally, the decisions will expand the size of most	17 February 2023	BIPA Tims v. Black Horse Carriers, Inc. Cothron v. White Castle Systems

	classes as well as the number of violations for which companies will be responsible.		
The Biden Administration Released the National Cybersecurity Strategy	On March 1, 2023, the Biden Administration released its National Cybersecurity Strategy ("**Strategy**"). The Strategy emphasizes regulatory mandates and imposing liability, enhancing voluntary information-sharing, and development of best practices. The Strategy will particularly affect critical infrastructure and cloud service providers.	1 March 2023	National Cybersecurity Strategy
FTC Requires Consumer Refunds for Compromised Health Data	On March 2, 2023, the Federal Trade Commission ("**FTC**") announced a proposed consent order with BetterHelp, Inc., an online counseling platform that allegedly disclosed consumer health data to third-party advertising platforms. Notably, the proposed order requires the company to pay $7.8 million to consumers to settle charges that it revealed consumers' sensitive data with third parties for advertising after promising to keep such data private. This is the first Commission action returning funds to consumers whose health data was compromised. This case highlights the high degree of scrutiny the FTC is applying to the processing of health-related information, and the FTC's increased willingness to bring unfairness claims.	2 March 2023	FTC Press Release Proposed Consent Order
CFPB Requests Information About Data Brokers for Planned Rulemaking	On March 15, 2023, the Consumer Financial Protection Bureau ("**CFPB**") announced that it is issuing a Request for Information about the business practices of data brokers, to assist it in planned rulemaking under the Fair Credit Reporting Act ("**FCRA**"). The CFPB has explained it is seeking information on (1) "new business models that sell consumer data," including information relevant to assessments of whether companies using these new business models are covered by the FCRA, and (2) "consumer harm and any market abuses, including those that resemble harms Congress originally identified . . . in passing the FCRA."	15 March 2023	Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information
California's CPRA Rulemaking Focuses in on Automated Decision-Making Tools	On March 27, 2023, the California Privacy Protection Agency ("**CPPA**") closed its second phase of rulemaking on automated decision-making ("**ADM**") systems under the California Privacy Rights Act ("**CPRA**")— but not before giving stakeholders an	27 March 2023	Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments,

	opportunity to help shape this important rulemaking around how businesses may use ADM systems and the scope of related consumer rights. The CPPA invited pre-rulemaking comments in response to a series of questions designed to inform its crafting of regulations on ADM. Aiming to balance the promotion of business opportunities against consumer protection, the CPPA is looking to better understand existing laws, assessments, and best practices, as well as which ADM technologies businesses and organizations already use, what they are doing to navigate existing laws, requirements and expectations. The Agency has additionally solicited input on the existing and potential consumer experience and impact created by the laws, requirements and practices to which CPRA-covered businesses are already subject.		and Automated Decision making
California's Office of Administrative Law Approves the CPPA's First Substantive Rulemaking Package for Further Implementation of CCPA Regulations	On March 30, 2023, the California Privacy Protection Agency ("**CPPA**") finalized their first substantive rulemaking package to further implement the California Consumer Privacy Act ("**CCPA**"), which was approved by the California Office of Administrative Law ("**OAL**"). The approved regulations are effective immediately. The approved regulations update existing CCPA regulations to harmonize them with amendments adopted pursuant to Proposition 24, the California Privacy Rights Act ("**CPRA**"); operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand. They place the consumer in a position where they can knowingly and freely negotiate with a business over the business's use of the consumer's personal information.	29 March 2023	
Plaintiffs' Attorneys Discover a New Tool in New York City Biometrics Law	Plaintiffs have filed two putative class action complaints in 2023, alleging violations of New York City's relatively new biometric information privacy law, signaling a new potential avenue for class action plaintiffs' to seek statutory damages from companies that collect, use, or store biometric information of their customers, consumers, and members of the general public. Enacted in 2021, NYC Admin. Code §§ 22-1201–1205 (the NYC Biometrics Law) requires covered commercial	30 March 2023	NYC Biometrics Law

	establishments that collect, store, convert, retain, or share customers' biometric identifier information to disclose the practice in "plain [and] simple language" on "clear and conspicuous" signage near establishment entrances. The law also prohibits such establishments from selling, leasing, or otherwise profiting from consumers' biometric information. It also provides the right to customers aggrieved by violations of the foregoing provisions to sue for statutory damages ranging from $500 to $5,000 per violation. Almost two years after its enactment, plaintiffs have only now begun to pursue recovery of these damages through the courts. In the second lawsuit of its kind, against the same company, a recently filed putative class action alleges that a large e-commerce company failed to properly notify customers that it used biometric identification technology in its cashier-less convenience stores across New York City. Class actions brought under comparable biometrics laws (most notably the Illinois Biometric Information Privacy Act) have led to extraordinary settlements and verdicts, sometimes reaching into the tens or even hundreds of millions of dollars. It remains to be seen whether the NYC Biometrics Law will be the vehicle behind a similar surge of privacy class actions.		
State-backed Cyber Attacks and Trends in Cyber Policies and Risk Management	On 16 August 2022, Lloyd's of London (Lloyd's) released Market Bulletin Y5381, which required that Lloyd's syndicates include certain baseline exclusions for state-backed cyberattacks in their policies from 31 March 2023 at the inception or on renewal of each policy. This requirement is part of a recent trend of limiting cyber incident coverage, as insurers attempt to limit their exposure for cyber incidents by raising premiums, limiting policy coverage and excluding coverage for certain events. It remains to be seen the extent to which Lloyds's decision to exclude state-backed cyber-attacks from standard cyber insurance policies will be mimicked by other insurance providers. However, Marsh Insurance initially published a critique of the exclusion requirement shortly after it was published. It then softened its stance and suggested its own exclusion language some weeks later, perhaps indicating the direction of travel. From the insurance industry's perspective, it is possible that some of the risk of state-backed attacks are shared with the	31 March 2023	Lloyd's Market Bulletin Y5381 Marsh Insurance Critique Marsh Insurance Exclusions

public sector, as happens with other risks such as terrorism and the pandemic, and this is something which has already been called for by certain insurers. For organizations, the time may come for executives and their Boards to re-examine whether and to what extent premium payments should be re-allocated to self-insurance, captives and improving preparedness, both from an IT and a governance perspective.



For further information, please contact:

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

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

@ESPrivacyLaw

Editorial Team:

Carolyn Sullivan
Associate
T: +44 20 7919 0941
carolynsullivan@eversheds-sutherland.com

Sophie Lewis
Trainee Solicitor
T: +44 20 7919 0944
sophielewis@eversheds-sutherland.com

Finn Potter
Trainee Solicitor
finnpotter@eversheds-sutherland.com

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

eversheds-sutherland.com

CLOUD_UK\212067826\4