EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

October to December 2022

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 **October to December 2022** and is full of newsworthy items from our team members around the globe, including:

- key legislative updates in relation to the EU-wide Digital Services Act and the NIS2 Directive, Switzerland's upcoming requirements for appointment of Swiss representatives and the anticipated implementation of the Swiss Information Security Act, as well as new legislation in China to regulate "deepfake" technologies and in the U.S., amendments to Pennsylvania's state data breach notification law;
- a renewed focus on marketing, with new direct marketing guidance and resources published in the UK and guidelines on the sale of customer databases in France. There's also been confirmation in South Africa that its new Enforcement Committee is handling numerous direct marketing complaints;
- developments on the lawful use of cookies, which is getting significant attention across various countries including Austria, Belgium, Germany and Slovakia, as well as the U.S.;
- developments in the field of data security/cybersecurity, including various new national standards for information security in China, the emergence of new national cybersecurity strategies in the Netherlands and the launch of an internet hygiene portal in Singapore;
- increasing volume of significant caselaw and published regulator investigations in France, Hong Kong, Germany, Ireland, the Netherlands and Poland. More specifically, we've seen also seen a number of courts passing judgment on the "right to be forgotten", with relevant cases emerging in Austria, Belgium and Sweden;
- additional published guidance on international transfer risk assessments in the UK and in China, new guidelines on security accreditation for cross-border transfers of personal data; and
- details of US President Biden's Executive Order intended to help re-establish an EU-U.S. framework for international transfers of personal data from the EU to the U.S.

Follow us on Twitter at:

@ESPrivacyLaw

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

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

General EU and International

Contributors

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

Jonathan Palmer
Senior Associate
T: +44 20 7919 4879
jonathanpalmer@
eversheds-sutherland.com

Development	Summary	Date	Links
European Council adopts Digital Services Act	Following on from the European Parliament's adoption of the Digital Services Act ("**DSA**") earlier this year, the European Council has now formally adopted the DSA as of 4 October 2022. The DSA aims to create a safer and more accountable online environment by imposing obligations on providers of online intermediary services (including online marketplaces and social media), increasing obligations around transparency and accountability. The European Council explains that: *"Amongst other things, the DSA:* – *lays down special obligations for online marketplaces in order to combat the online sale of illegal products and services;* – *introduces measures to counter illegal content online and obligations for platforms to react quickly, while respecting fundamental rights;* – *better protects minors online by prohibiting platforms from using targeted advertising based on the use of minors' personal data as defined in EU law;* – *imposes certain limits on the presentation of advertising and on the use of sensitive personal data for targeted advertising, including gender, race and religion;* – *bans misleading interfaces known as 'dark patterns' and practices aimed at misleading"* Larger providers with 'significant societal impact' are subject to stricter rules under the DSA and may be subject to a shorter transitional period than other smaller providers.	4 October 2022	European Council Press Release
EU adopts NIS2 Directive	The EU Parliament and the Council of the EU have each **adopted** the NIS2 Directive (Directive on measures for a high common level of	10 November 2022	European Council Press Release

Development	Summary	Date	Links
	cybersecurity across the Union, repealing Directive (EU) 2016/1148) which will replace the existing EU NIS Directive. NIS2 is intended to address deficiencies in the current NIS Directive, including by: – expanding its scope to apply to more sectors (based on their criticality for the economy and society) and introducing a size cap rule to identify regulated entities – removing the distinction between operators of essential services and digital service providers and replacing this with a new system that will classify in-scope entities as essential or important, with a different regime for each category – requiring in-scope organisations to address cybersecurity risk in their supply chains – establishing the European Cyber Crises Liaison Organisation Network to support coordinated management of large-scale cybersecurity incidents and crises – aligning with sector specific legislation including DORA and the directive on the resilience of critical entities NIS2 will enter into force 20 days after being published in the OJEU. EU member states will then have 21 months in which to implement it. Organisations that fall within the scope of both NIS2 and the UK NIS regime will then be required to comply with divergent rules.		
New Liability Rules for AI Products	The European Commission has published two proposals aimed at updating product liability rules for the digital age. The two Directives are also said to align with the objectives of the European Commission's White Paper on AI and 2021 AI Act proposal, setting out a framework for excellence and trust in AI. The two Directives proposed are: **Product Liability Directive ("PLD")** The PLD adapts existing product liability rules to address compensation for defective products emerging from new digital technologies, like smart products and artificial intelligence (AI). The PLD confirms that victims can claim compensation if software or AI systems cause damage, including personal injury. The proposed rules also apply to manufacturers and other businesses who modify or upgrade products already on the market.	19 October 2022	White Paper

Development	Summary	Date	Links
	AI Liability Directive ("AILD") The AILD seeks to ensure that victims of harm caused by AI technology can access reparation, in the same manner as if they were harmed under any other circumstances. The new rules introduce two main changes to achieve this: – Replacing the victims' "burden of proof" with "presumption of causality". Victims can show e.g. a manufacturer was at fault for not complying with a certain obligation relevant to the harm caused, and a causal link with the AI performance. Courts can presume in such a case that non-compliance with the obligation caused the damage. – Victims will have a right of access to evidence by obtaining a court order to disclose relevant and necessary evidence about high-risk AI systems (subject to appropriate safeguards). **Impact and actions** If approved, as well as clarifying the existence of liability for damage caused by AI, the PLD will require companies to disclose evidence that a claimant would need to prove their case in court, to address the information gap between consumers and manufacturers. Non-EU manufacturers must also have an EU based representative from whom consumers can seek compensation. The AILD means that providers of AI systems can be held liable for harm caused by AI technology where victims can prove a "causal link" between the damage caused and a failure by the provider to comply with certain obligations.		
Visitors to the World Cup in Qatar warned by EU supervisory authorities to pay close attention to their digital security	Individuals who visited the World Cup were required to install a number of applications on their mobile phone. The Dutch DDPA advised Qatar visitors to use a telephone that they do not use for anything else. The apps in question included a corona tracker app (Ehteraz) and a special World Cup app (Hayya). Privacy regulators from several European countries pointed out that the apps were likely to collect information about users without users being aware of it. For instance, the application collects data on the user's caller history, apps installed on the phone and possibly has access to the user's photos. Earlier in 2022, the German, French, Norwegian and Danish privacy regulators warned against the use of these apps. The German regulator in particular had carried out an analysis of the apps. The Dutch DDPA agreed with the previous warnings of its fellow European supervisory authorities.	17 November 2022	DDPA Statement (Dutch only)

General EU and International

Development	Summary	Date	Links
Nordic data protection authorities issue a joint declaration	In October 2022, representatives of all Nordic data protection authorities met in Helsinki. On the agenda was, among other things, strategic cooperation within the Nordic region. The meeting resulted in a joint declaration in which the data protection authorities state their willingness to continue working closely together to promote a safer and more responsible digital environment. The Nordic data protection authorities shall, inter alia, further contribute to the work of the European Data Protection Board (EDPB) in order to achieve a harmonised application of the GDPR. The protection of children's personal data is a priority for the Nordic data protection authorities. The DPAs decided to set up an informal working group related to children and online gambling to, among other things, exchange information and identify opportunities for joint guidance or enforcement actions. In the declaration, the Nordic data protection authorities flagged that the GDPR and other EU legislation related to digitalisation may overlap and emphasised the importance of avoiding undesirable fragmentation of supervision of these laws.	18 October 2022	Press statement (in Swedish) Declaration (in English)
European Commission approves next version of 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. The UK's Regulator, the ICO, has published new guidance on the use of AI in an effort to help regulators better understand it for the sectors it regulates. In the EU, the European Commission's AI Act ("**Act**") proposal has undergone further changes following review by EU member states. The Council of the EU approved a compromise version of the Act on 6th December 2022. The European Parliament are expected to vote on the draft by the end of March 2023, with a view to adopting the Act by the end of 2023. To read more about the changes made in the latest version of the Act, click the link titled 'Eversheds Sutherland Article' to reach our published article.	December 2022	ICO Guidance Eversheds Sutherland Article

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
Federal Administrative Court rules on permissibility of GPS tracking of company vehicles	Following an appeal against a decision by the Austrian Data Protection Authority, the Austrian Federal Administrative Court ruled on the permissibility of an employer using GPS technology to track company vehicles. The Court established that the use of such technology in an employment context is only permissible under strict requirements. Amongst others, data on *private* use of company cars may only be technically accessible in cases of car theft. GPS data must be deleted after 45 days at the latest unless a legitimate reason for longer retention applies. Furthermore, a Data Protection Impact Assessment is required.	Date of Decision: 25 August 2022 Published: 29 December 2022	Link to the decision (in German)
Austrian DPA: Processing of online user-ID and use of analytics and advertisement cookies requires prior consent	The Austrian DPA ruled against the operator of a website for sports equipment. While the website had a cookie-banner, it used analytics and advertisement cookies before the user interacted with the banner and even if no consent was given. Following this, data was shared with advertisement partners. The data included the visited product pages as well as unique user-IDs stored on the users' devices. The DPA ruled that such unique user-IDs are personal data and processing is subject to GDPR. As the cookies were not technically necessary and were placed without the user's consent, this was a violation of the Austrian implementation of	Date of Decision: 1 June 2022 Publication of summary in DPA's newsletter: 10 October 2022	Link to the summary in the DPA's newsletter (in German; the full text of the decision is not yet published)

Development	Summary	Date	Links
	the EU ePrivacy-Directive in the Austrian Telecommunications Act ("**TKG**"). Furthermore, the processing of the data collected via these cookies and the sharing of this data with the website's advertisement partners was considered a violation of GDPR, as no consent was obtained, and processing cannot be based on legitimate interest (Article 6 (1)(f) GDPR) if the data was collected in violation of the ePrivacy Directive and its local implementation which requires user consent. It is not known whether the decision is already legally binding or has been appealed.		
Federal Administrative Court: Acquittal in Criminal Court does not automatically grant the right to be forgotten against a search engine regarding reports on the allegations	The complainant was a former local politician in Austria. Criminal allegations were raised against him when he posted quotations on his social media profile which were derived from Nazi or far-right songs. Publication of Nazi material is prohibited in Austria. Many national and international media outlets reported on these allegations and the complainant's following dismissal by his political party. The complainant claimed that he had not been aware of the origin of the quotations. In court, the complainant was acquitted by the jury. Based on the 'right to be forgotten', the complainant then requested that the defendant search engine operator delete 67 links to media coverage of the allegations, claiming that they were factually wrong and unjustified. The search engine operator refused, which led to the complainant filing a complaint with the DPA. Whilst the DPA upheld the complaint for a small number of links, for the rest, the complaint was denied. Following an appeal to the Federal Administrative Court, the Court decided on the case. The Court, on the most part, upheld the DPA's decision. It argued that the mere fact that the complainant had been acquitted in the Criminal Court does not automatically lead to a 'right to be forgotten' regarding the reports on the allegations. A balancing of interests has to take place. In this individual case, as the complainant had been a local politician and thus a public figure and as it is clear – despite the acquittal – that he had posted the quotations in question, there was a public interest in the media coverage on the allegations and their consequences. This is particularly the case as it was not too long ago that the complainant had stopped acting as a politician. The complaint was upheld for one link, which led to a report that was clearly factually wrong, as it wrongly claimed that the complainant had been expelled from his political party.	Date of Decision: 20 July 2022 Published: 8 November 2022	Link to the decision (in German)

Austria

Development	Summary	Date	Links
Federal Administrative Court: Taking pictures as evidence for a future complaint does not violate GDPR	In this case, the Federal Administrative Court ruled on a complaint under GDPR. The defendant had taken pictures of the complainant's car in order to file a complaint to the police due to a parking violation. The Court ruled that whilst a car's license plate can be considered personal data, in this case there was a legitimate interest in collecting evidence for such a complaint. As there was no relevant overriding interest of the complainant, the processing was considered permissible under GDPR. The complaint was therefore denied.	Date of Decision: 23 September 2022 Published: 28 November 2022	Link to the decision (in German)
Austrian DPA issues quarterly newsletter	This edition of the Austrian DPA's quarterly newsletter focuses on the DPA's recently initiated inquiry into the permissibility of the dynamic use of web fonts under GDPR (see our last edition of Updata for more details on this inquiry). Furthermore, the DPA gives an update on its project "privacy4kids - Rising awareness about privacy of children in the digital age", an EU funded project aimed at creating and publishing educational videos on privacy and data protection for children between the ages of 6 and 14. The creation of further educational material is planned.	10 October 2022	Link to the newsletter (in German) Link to the website of the project "privacy4kids" (in German)
Austrian Ministry of the Interior invites Public Authorities to a Cyber Security Conference	Following a major cyber-attack on the IT systems of the Austrian state of Carinthia in the summer of 2022 and other recent attacks on regional entities, the Austrian Ministry of the Interior and the state of Carinthia conducted a Cyber Security Conference for Public Authorities in November 2022. The goal of the conference was to raise awareness of cyber risks, to share experiences and to inform representatives of the correct approach in case of a cyber security breach. This conference shall be repeated regularly in subsequent years.	7 November 2022	Link to press release (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 DPA rules on the principle of data minimization in identification verification procedure	A data subject submitted a request to erase their personal data, upon which the controller asked to transfer a proof of their identity. This was also foreseen in the controller's privacy notice. The Belgian Data Protection Authority (the "**DPA**") ruled that this infringed Article 5.1 (c) GDPR - from which the principle of data minimization is derived – as the controller already had sufficient personal data to fulfil the request of the data subject. More specifically, the controller had previously obtained the data subject's e-mail address in the context of direct marketing messages which the DPA found to be sufficient to identify the data subject in order to fulfil the request of data erasure. As it was the controller's first infringement, the controller was not issued with a fine, and was asked to inform the DPA in 30 days of the changes made to its privacy notice.	12 October 2022	Decision (Dutch)
Belgian DPA issues several settlement proposals after investigations into the use of cookies on Belgian news websites	In our contribution to Updata Edition 16, we have discussed that the DPA is carrying out large-scale investigations on 20 Belgian news websites in relation to their cookie banners. Two administrative fines of EUR 50,000 each had been imposed at that time: one on the press group Roularta, and another one on the press group Rossel. The DPA has now issued several settlement proposals in relation to its investigation. This implies that the DPA will not find an infringement of the GDPR in these cases and they will formally close the case, in exchange of a payment of EUR 10,000 by the relevant controller. Furthermore, the controller shall have to waive any civil or other action with regard to the settlement.	Date of Decisions n° 150/2022 and 151/2022: 12 October 2022 Date of Decisions n° 153/2022, 154/2022, 155/2022, 156/2022 and 157/2022: 4 November 2022	Decision n° 150/2022 Decision n° 151/2022 Decision n° 153/2022 Decision n° 154/2022 Decision n° 155/2022 Decision n° 156/2022 Decision n° 157/2022

Development	Summary	Date	Links
	We consider this to be a very interesting development as it is the first time that this type of settlement decision has been proposed by the Belgian DPA.		
Market Court overturns the decision of the Belgian DPA in a case against a search engine operator on the erasure of links in searches	In our contribution to Updata Edition 15, we explained the decision of the Belgian DPA concerning a search engine operator's refusal to delete/'de-list' certain disputed links, and therefore, to not grant a complainant's request for erasure. The Belgian DPA eventually dismissed the complaint for technical reasons but still issued a reprimand on the Belgian entity of the search engine operator because it allegedly breached Articles 12.1 and 12.2, in conjunction with Article 17 GDPR. The reasoning behind the decision was that although each reply of the relevant search engine operator entity contained a link to the correct form to be used in a request for erasure, the process could still confuse a complainant. This confusion arose because the different entities of the search enginge operator all successively referred to another entity of the search enginge operator which should be responsible. According to the Belgian DPA, the complainant could not reasonably be expected to know the roles and responsibilities of each of the search engine's entities. The Belgian and US entities of the search engine operator have appealed this decision to the Market Court. On 26 October 2022, the Market Court overturned the part of the decision of the DPA which relates to the reprimand on Belgian entity.	26 October 2022	Decision (French)
Belgian DPA announces its priorities for 2023 to the Chamber of Representatives	Provided sufficient resources are available, the DPA will focus its efforts in 2023 on: – Cookies: by striving to make its position on cookies more explicit, as a harmonised position at European level is currently lacking. This does not come as a surprise, given, e.g., the two recent fines of EUR 50,000 and the various settlement proposals of EUR 10,000 for news websites (see above). – Data processing officers (DPOs): by supporting the role of DPOs, both in terms of preventive actions (in particular, through highlighting the DPO's role in exercising the rights of complainants), and in terms of supervision (for example, the Inspectorate of the DPA will examine the place of the DPO in organisations under investigation). – Smart cities: by developing prevention actions and engaging with local actors in the field of smart cities (e.g., intelligent transport).	15 November 2022	Press release (Dutch) Press release (French)

Development	Summary	Date	Links
	– Youth awareness: the DPA would like to continue the successful awareness-raising project "I decide" ("ik beslis"/ "je decide"), targeting young people on the one hand and parents and teachers on the other hand. In addition to these common concerns for all DPA bodies, the various bodies will be able to identify priorities specific to their services for the coming year, particularly on the basis of recurring requests for information or complaints. For example, the Inspectorate and the Litigation Chamber will continue to investigate and, if necessary, impose sanctions on data brokers, who often process personal data on a very large scale.		

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

Information Security Technology — Basic Security Requirements for Pre-installed Applications on Smartphones (Draft for Comments)
《信息安全技术 智能手机预装应用程序基本安全要求（征求意见稿）》
	On 9 October 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, the Information Security Technology — Basic Security Requirements for Pre-installed Applications on Smartphones (Draft for Comments) (the "**Draft**"), for public consultation until 8 December 2022.
	
	The Draft sets out the basic security technology and security management requirements for pre-installed and third-party pre-installed applications as follows:
	
	– Data security requirements for pre-installed applications:
	  – collection of personal information must comply with the 'Information Security Technology - Basic Specification for Collecting Personal Information in Mobile Internet Applications (App)';
	  – the application should only request relevant system and personal information permissions *after* users begin interacting with the application;
	  – for applications that cannot be uninstalled, a "stop using" function shall be provided for users to stop the processing of their personal information; and
	  – separate consent shall be obtained to transfer sensitive personal information out of the smartphone.
		9 October 2022	National standard (draft bill) (in Mandarin)

Development	Summary	Date	Links
	– Managing security of third-party pre-installed applications: Smartphone manufacturers are responsible for reviewing the data security and personal information protection capacity of third-party pre-installed application providers and the applications' personal information processing rules. Also, simple and accessible complaint and reporting channels should be set up to ensure prompt handling of users' feedback on security issues related to such applications.		
Information Security Technology—Cybersecurity Requirements for Critical Information Infrastructure Protection **《信息安全技术 关键信息基础设施安全保护要求》**	On 12 October 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, the Information Security Technology—Cybersecurity Requirements for Critical Information Infrastructure Protection (the "**Standard**"), which will come into force on 1 May 2023. The Standard provides that critical information infrastructure ("**CII**") security protection is based on the cybersecurity multi-level protection scheme. The relevant requirements are categorized into six main areas and include, but are not limited to, the following: – Analysis and Identification: CII operators should conduct business, asset and risk identification focusing on key businesses and/or critical business chains of CII, and conduct re-identification where there is substantial change. – Security Protection: the Standard sets out requirements for a security management system, organization, personnel, communication network, computing environment, infrastructure management, supply chain, etc. For example, CII operators shall establish a cybersecurity working committee or leadership group, with one member being the chief cybersecurity officer. A responsible person with relevant capabilities and qualifications shall also be assigned for each CII. The safety of a supply chain shall be ensured by creating an annual list of purchased network products and services, executions of confidentiality agreements with the suppliers, and obtaining a license to use supplier's IP rights, etc. – Assessment and Evaluation: CII operators shall themselves conduct, or entrust cybersecurity service organizations to conduct, assessments and evaluations at least once a year, or regularly organise or participate in cross-CIIs security assessments. – Monitoring and early warning: CII operators shall formulate and implement cybersecurity monitoring, warning and information notification systems and establish information sharing mechanisms with regard to cybersecurity threats to improve their ability to proactively detect attacks.	12 October 2022	National Standard (in Mandarin)

Development	Summary	Date	Links
	– Proactive defense: CII operators shall enhance their identification, analysis and defense abilities in relation to cyber threats and attacks. – Incident Handling: CII operators shall formulate emergency plans and organize emergency drills at least once a year. Where a cybersecurity incident occurs, appropriate responses shall be adopted to handle the incident and restore damaged functions or services, and a report of the incident shall be produced.		
Information Security Technology — Security Requirements for Processing of Motor Vehicle Data **《信息安全技术 汽车数据处理安全要求》**	On 14 October 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, Information Security Technology — Security Requirements for Processing of Motor Vehicle Data (the "**Standard**"), which will take effect from 1 May 2023. The Standard sets out the security requirements for (i) general processing of motor vehicle data (i.e. personal information data and important data involved in the design, manufacturing, sales, usage and maintenance of motor vehicles), (ii) vehicle's external data and (iii) cabin data. The key security requirements are summarized below: – Personal information: the data subject shall be expressly informed of the specific retention period and storage location of their personal information through the user manual, audio playback, a pop-up window in the car monitor, etc. Personal information shall be anonymized or de-identified before conducting other processing activities. – Sensitive personal information: separate consent shall be obtained for processing each item of sensitive personal information (i.e. consent cannot be obtained all at once for multiple items of sensitive personal information or processing activities). The duration of consent shall not be "always permitted" or "permanent". A record shall be established to ensure use of sensitive personal information is traceable. Continuous collection of sensitive personal information shall be indicated through distinct and clear methods such as the blinking of certain icons on a car monitor, or of the signalling device indicator light. – Localization of data: personal information involving cabin data, location tracking data, video/graphical data collected from outside of the vehicle, and personal information with a quantity exceeding 100,000 people shall be stored within the territory of PRC according to the relevant laws. – Vehicle's external data: such data shall not be provided outside of the vehicle until after anonymization, by deleting the whole or part of	14 October 2022	National standard (in Mandarin)

Development	Summary	Date	Links
	the videos or graphics such that they cannot be linked to the personal information subject. – Cabin data: the default mode of the vehicle should be that cabin data is not collected (including not turning on camera, microphone, etc.). Collection of such data shall require the driver to perform a certain act, such as pressing a button, and shall be easily terminated by the driver. Further, motor vehicle data processors are required to conduct a security assessment, appoint a responsible person for data security management, establish an emergency processing system and a complaint handling mechanism.		
Administrative Provisions on Security of Personal Information of Postal and Delivery Users (Draft for Comments) **《寄递用户个人信息安全管理规定（征求意见稿）》**	On 25 October 2022, the State Post Bureau issued the Administrative Provisions on Security of Personal Information of Postal and Delivery Users (Draft for Comments) (the "**Draft**"), for solicitation of public comments until 23 November 2022. The Draft is applicable to the operation and use of postal and delivery services (the "**Service**") within the People's Republic of China which involves Service users' personal information and is subject to the supervision and management of postal management departments. The key points of the Draft are summarized as follows: – Scope of personal information: Postal and delivery service user personal information is identified as the information recorded by the users during their use of the Service. This includes, for example, the sender and receiver's name, ID number, address, phone number, unit name, personal biometric information, delivery note number, time, item details, etc. – General responsibilities of postal and delivery enterprises: the enterprises shall only collect users' personal information to the extent necessary to complete the Service. The postal and delivery enterprises must also enter into a confidentiality agreement with their staff to ensure that users' personal information remains confidential. The enterprises must conduct a personal information protection impact assessment on any entrusted third parties they engage, monitor their personal information processing activities, and bear relevant responsibilities for leakage, falsification and loss of personal information. A complaint handling and response system should also be set up. The enterprises shall (and shall request any entrusted third parties they enage to) de-identify the delivery note information to prevent leakage of such information during the delivery.	25 October 2022	New legislation (draft bill) (in Mandarin)

Development	Summary	Date	Links
	– Supervision of Cyberspace Administration of China ("**CAC**"): the relevant rules and regulations must be complied with where the quantity of personal information processed reaches the CAC benchmark, or in circumstances where the enterprises are required to transfer users' personal information overseas due to business needs.		
Implementation Rules for Personal Information Protection Accreditation **《个人信息保护认证实施规则》**	On 4 November 2022, the Cyberspace Administration of China and the State Administration of Market Regulation issued the Implementation Rules for Personal Information Protection Accreditation (the "**Rules**"), which applies with immediate effect on the certification of (i) collection, storage, use, processing, transmission, provision, disclosure and deletion of, and (ii) cross-border transfer of, personal information. Pursuant to the Rules, the certification process includes: – Engaging an accreditation institution to confirm the accreditation plan according to the information provided on the type and quantity of personal information, scope of processing, and other information; – Technical verification conducted by a technical verification institution based on the accreditation plan and issuance of technical verification report; – On-site examination by the accreditation institution and issuance of on-site examination report; – Evaluation by the accreditation institution based on the materials provided by the applicant, technical verification report, on-site examination report, and issuance of accreditation certificate where the requirements are met; and – Continuous post-accreditation supervision by the technical verification institution during the valid term of certificate. A personal information accreditation certificate is valid for three years and can be altered, cancelled, revoked, or suspended during the period. If renewal is necessary, an application should be submitted within six months of the expiry.	4 November 2022	New legislation (in Mandarin)
Opinions on Promotion of Standardized and Sound Development of Cybersecurity Insurance (Draft for Comments)	On 7 November 2022, the Ministry of Industry and Information Technology issued its Opinions on Promotion of Standardized and Sound Development of Cybersecurity Insurance (Draft for Comments) (the "**Draft**"), for public consultation until 18 November 2022. The Draft aims to: accelerate the integration and development of cybersecurity industry and financial services, develop a new model of cybersecurity insurance, enhance cybersecurity risk management of	7 November 2022	Draft opinion (in Mandarin)

Development	Summary	Date	Links
《关于促进网络安全保险规范健康发展的意见（征求意见稿）》	enterprises and promote high-quality developments within the cybersecurity industry. The key points of the Draft are summarized as follows: – Cybersecurity insurance policy standard system: the Draft focuses on improving the insurance policy system and the establishment of a set of relevant standard guidelines on a number of topics including application and underwriting, quantitative assessment of cybersecurity risks and risk monitoring. – Innovative development of cybersecurity insurance products and services: the Draft encourages development of diversified products with respect to different industries and enterprises, with the aim of reducing cybersecurity risk and also encourages cooperation amongst insurance service organizations to explore cybersecurity risk management solutions. – Strengthening relevant technology: quantitative assessment of cybersecurity risks shall be carried out and relevant models, assessment and analysis tools shall be explored and developed. Cybersecurity risk monitoring capabilities will also be enhanced with the use of technology to promptly discover pertinent risks and dangers. – Enhancing the supply of cybersecurity insurance services: the Draft aims to improve cybersecurity risk response capabilities of enterprises, in particular SMEs, with the use of cybersecurity insurance tools and security protection of network infrastructure.		
Information Security Technology - Capability Requirements of Cybersecurity Service (Draft for Comments) **《信息安全技术 网络安全服务能力要求（征求意见稿）》**	On 9 November 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, Information Security Technology - Capability Requirements of Cybersecurity Service (Draft for Comments) (the "**Draft**"), for solicitation of public comments until 9 December 2022. The Draft outlines the specific requirements on the capabilities that cybersecurity service providers must possess and will replace the existing 'Information Security Technology – Management Requirements of Information Security Service Providers' once the Draft comes into effect. The key changes made by the Draft are as follows: – Definition: The Draft replaces the term "information security service" with "cybersecurity service", which is defined as the process of providing a service to a cybersecurity service acquirer based on technical resources such as service personnel, tools and management systems in accordance with the service agreements.	9 November 2022	National Standard (Draft Bill) (in Mandarin)

Development	Summary	Date	Links
	– General requirements: A cybersecurity service provider must be registered within the People's Republic of China and shall not be listed in any serious untrustworthy list that may affect the provision of cybersecurity service. The Draft also sets out new requirements on supply chain management, remote services, legal protection, data protection, continuity of service, etc. – Special requirements: New special requirements on evaluation and testing assessments, security maintenance, security consultation, and disaster recovery are set out under Chapter 6 of the Draft with regard to different types of cybersecurity services.		
Administrative Provisions on Internet Comment Posting Services **《互联网跟帖评论服务管理规定》**	On 16 November 2022, the Cyberspace Administration of China issued the revised Administrative Provisions on Internet Comment Posting Services (the "**Revised Provisions**"). The Revised Provisions came into effect on 15 December 2022. The Revised Provisions clarify the management responsibilities of comment posting service providers ("**Service Providers**"), which include conducting authentication of users' real identity information, establishing personal information protection systems, reviewing the contents of comment posts on news before publication, etc. Service Providers are required to conduct standardized management of their service users, public account producers and operators in compliance with the user service agreement and establish a user management categorization system. In addition, Service Providers shall set up a complaint system for the public and service users and must promptly handle such complaints. The Revised Provisions also expand the scope of the security assessment that Service Providers with the ability to influence public opinion or social mobilization are required to conduct. The security assessment must be carried out in accordance with the relevant regulations. "**Likes**" are also regarded as comment posts under the Revised Provisions. The Revised Provisions further set out the obligations of comment posting service users with regard to the information that they publish. Public account producers and operators shall enhance the review and management of their comment posting section, discover any unlawful acts promptly, including indecent information, and take necessary measures.	16 November 2022	Revised legislation (in Mandarin)
Information Security Technology — Framework for Cybersecurity Emergency System of Critical Information Infrastructure (Draft for Comment)	On 17 November 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, Information Security Technology — Framework for Cybersecurity Emergency System of Critical Information Infrastructure (Draft for Comment) (the "**Draft**"), for solicitation of public comments until 16 January 2023.	22 November 2022	National standard (draft bill)

Development	Summary	Date	Links
《信息安全技术 关键信息基础设施网络安全应急体系框架（征求意见稿）》	The Draft provides guidance for critical information infrastructure operators ("**CIIO**") on the set up of cybersecurity emergency systems and how to carry out cybersecurity response. The Draft focuses on a number of key topics including: the establishment of cybersecurity management organizations, formulation of cybersecurity emergency plans based on identification of critical business, monitoring and early warning, emergency response/handling, post-cybersecurity incident recovery and analysis, incident report and information sharing, emergency protection, and drills and training.		
Administrative Provisions on Deep Synthesis of Internet Information Services **《互联网信息服务深度合成管理规定》**	On 25 November 2022, the Cyberspace Administration of China, together with the Ministry of Industry and Information Technology and Ministry of Public Security, issued the Administrative Provisions on Deep Synthesis in Internet Information Services (the "**Provisions**"), which came into effect on 10 January 2023. The Provisions apply to circumstances where Internet information services are provided using deep synthesis technology (commonly known as "deepfake" technology) within the territory of the People's Republic of China. The key points of the Provisions are summarized as follows: – Deep synthesis technology: Deep synthesis technology refers to any technology that employs deep learning, virtual reality or any other generative or synthetic algorithm to produce text, images, audio, video, virtual scenes or other network information, including but not limited to generation/editing of text content, speech content, music or scene sound, face or posture, image, digital characters and virtual scenes. – General obligations of deep synthesis service providers ("**Service Providers**"): Service Providers shall (i) authenticate the real identity of service users and shall not provide information release services to users whose real identity has not been verified; (ii) set up a feature database to identify and prohibit illegal and unhealthy contents and retain relevant network logs; (iii) review data input and synthesized results and keep the relevant records; (iv) report to cyberspace authorities and take relevant disposition measures where any illegal and unhealthy content is discovered; and (v) establish a complaint handling system and an anti-rumor mechanism. – Specific requirements: Where Service Providers or technical supporters (i.e. organizations or individuals that provide technical support for the Services) provide Services that edit biometric information such as faces and voices, the data subject's separate consent shall be obtained. If the Services contain functions that generate or edit biometric information, or may involve national security, state image, state interests and social public interests, a	25 November 2022	New Legislation (in Mandarin)

Development	Summary	Date	Links
	security assessment shall be performed. For Services that may cause any confusion or misrecognition to the public, the Service Provider must disclose the circumstances of deep synthesis by placing a prominent mark at a reasonable position of the generated/edited information. Service Providers with the ability to influence public opinion or social mobilization shall also conduct algorithm record filing and security assessments of new products in accordance with the relevant laws.		
Industrial Internet Enterprise Cyber Security Part 4: Protection Requirements of Data (Draft for Comment) **《工业互联网企业网络安全 第4部分：数据防护要求（征求意见稿）》**	On 1 December 2022, the National Information Security Standardization Technical Committee issued a recommended national standard, Industrial Internet Enterprise Cyber Security Part 4: Protection Requirements of Data (Draft for Comment) (the "**Draft**"), for solicitation of public comments until 30 January 2023. The Draft sets out the security protection procedures and requirements, and security management requirements for different levels of industrial internet data. The key points of the Draft are summarized as follows: – Data security protection requirements: Once industrial internet data assets are discovered, the data processor shall classify and grade such data and manage and protect the data accordingly. An overall data classification and grading list, in addition to specific catalogues for important data and core data should be created. The Draft also specifies the relevant requirements for the acquisition, storage, processing, transfer, public disclosure and destruction provision of ordinary data, important data and core data. – Data security management requirements: The Draft sets out the requirements for the security management organization and system, personnel, equipment security, authorization, and supply chain security, monitoring, information sharing, and emergency responses. Data processors are also required to carry out a security assessment, retain a log and conduct a security audit. Important data and core data processors are subject to more requirements than ordinary data processors.	1 December 2022	National standard (draft bill) (in Mandarin)
Circular on the Issuance of Typical Cases of the Procuratorate's Punishment of Crimes Infringing on Citizens' Personal Information **《关于印发检察机关依法惩治侵犯公民个人信息犯罪典型案例的通知》**	On 2 December 2022, the Supreme People's Procuratorate issued a Circular on the Issuance of Typical Cases of the Procuratorate's Punishment of Crimes Infringing on Citizens' Personal Information (the "**Circular**"). The Circular emphasizes that the procuratorate at all levels shall enhance the performance of their duties and dismantle the entire chain of personal information-related criminal activities. The Circular sets out five typical cases which demonstrate an infringement of the law for various types of personal information, such as citizen's	2 December 2022	Typical Cases (in Mandarin)

Development	Summary	Date	Links
	credit information, biometric information, location tracking information, and health and physiological information. The Circular reinforces and clarifies the legal questions relating to the enforcement of personal information laws. For example, according to the first typical case, the illegal acquisition and sale of citizens' credit information should be charged and punished as the crime of infringement of citizens' personal information where the circumstances are serious (based on the quantity of information or amount of illegal income); the fourth typical case held that illegal sale or provision of credit information that is used to conduct crimes is serious in nature and constitutes the crime of infringement of citizens' personal information.		
Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation) **《工业和信息化领域数据安全管理办法（试行）》**	On 8 December 2022, the Ministry of Industry and Information Technology ("**MIIT**") issued the Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation) (the "**Measures**"), which came into effect on 1 January 2023. The Measures regulate the data processing activities and data security in the industrial and information technology sector within the territory of the People's Republic of China. This marks the move towards a comprehensive industry-wide regulation for industrial and information technology data. The key points of the Measures are summarized as follows: – Scope: Data in the industrial and information technology sector ("**Industrial and IT Data**") includes industrial data, telecommunication data, and radio data. – Data classification and grading: The MIIT will formulate standards and specifications for data classification and grading, the identification of important data and core data and issue a specific catalogue of important data and core data. According to the standards and specifications, the local industry regulatory authorities shall organize for classification and grading of data in its jurisdiction. Industrial and IT Data shall be categorized according to the industry requirements, characteristics, business demands, data sources, purposes, etc. The categories include, but are not limited to, research and development data, production and operation data, management data, operation and maintenance data, and business service data. The grading and classiciation will be based on the extent of potential harm that could be caused to national security, public interests, or the legitimate rights and interests of individuals and organizations by the tampering, destruction, disclosure, illegal acquisition, or illegal use of such data. Industrial and IT Data is	8 December 2022	New Legislation (in Mandarin)

Development	Summary	Date	Links
	generally divided into three grades: general data, important data, and core data. – Catalogue filing: Processors of Industrial and IT Data are required to file a catalogue of important and core data with the local industry regulatory authorities, which will complete the review of such application within 20 working days. Where the filing fulfills the relevant requirements and is approved, it shall be reported to the MIIT. In cases of material changes to the contents filed (i.e. changes of more than 30% in the scale of certain important and core data (e.g. number of data entries, total storage amount), or changes in other filed content), the data processor shall perform the filing procedures for changes within 3 months of the change. – Data processor obligations: The Measures also set out the general data security obligations of data processors, such as establishing a full life cycle data security management system, designating data security personnel, formulating emergency plans, and so on. Processors of important and core data are subject to additional security requirements.		
Network Security Standard Practice Guidelines – Guidelines on Security Accreditation for Cross-border Processing of Personal Information V2.0 **《网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0》**	On 16 December 2022, the National Information Security Standardization Technical Committee issued the Network Security Standard Practice Guidelines – Guidelines on Security Accreditation for Cross-border Processing of Personal Information V2.0 (the "**New Guidelines**"). The New Guidelines amend and further detail the accreditation requirements for cross-border transfers of personal information made under the Network Security Standard Practice Guidelines – Guidelines on Security Accreditation for Cross-border Processing of Personal Information V1.0 ("**Guidelines V1.0**"). The key amendments are summarized as follows: – Application Scope: the New Guidelines remove the limitation on the applicable scope under Guidelines V1.0. The amendment provides that the accreditation mechanism shall apply to all personal information processors conducting cross-border personal information transfer. The New Guidelines also require the personal information processors to be a qualifying legal person (i.e. an organisation/entity with an independent legal status (excluding branch and representative offices)), conduct normal operations and have a good reputation. – Obligations of overseas recipients: overseas recipients are required to undertake further responsibilities that are similar to those undertaken by a personal information processor ("**PIP**"), specifically in relation to the fundamental principles, legal agreements, and	16 December 2022	New Guidelines (in Mandarin)

Development	Summary	Date	Links
	liability. Overseas recipients are also obliged to (i) promptly notify the PIP and the accreditation organization of any change to their local laws or policies in their country or jurisdiction that render it impossible to fulfill requirements under the accreditation; (ii) not provide the personal information received to any other third party, or where such provision is required, take necessary measures to ensure that the third party complies with the standards under Personal Information Protection Law of the People's Republic of China; and (iii) retain records of its cross-border personal information processing activities for at least the last 3 years. – Legal document: the New Guidelines provide further details on the contents of the cross-border transfer agreement between the PIP and overseas recipient (collectively, "**Parties**"), which are in line with those stipulated under the draft Provisions on Standard Contract for Cross-Border Data Transfer and Measures on Security Assessment of Data Export. – Responsibilities of personal information protection organizations: personal information protection organizations established by the Parties shall also be responsible for (i) conducting periodic compliance audits and (ii) accepting supervision by accreditation organizations, including answering queries and cooperating with inspections. – Personal information protection impact assessment ("**PIPIA**"): the New Guidelines articulate additional details as to the contents of the PIPIA report, which again align with those stipulated under the draft Provisions on Standard Contract for Cross-Border Data Transfer. Also, the PIPIA report should be kept by the PIP for at least 3 years.		

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
Czech Government finally approves substantially revised draft of Whistleblowing Law	On 23 November 2022, a new draft law on the Protection of Whistleblowers implementing the Whistleblower Directive (Directive (EU) 2019/1937) (the "**Bill**") has been approved by the Czech government. The Bill is limited in material and personal scope as follows: – reports on all administrative offences no longer fall under the Bill, limiting the scope of the Bill only to offences which bear the characteristics of a crime or a breach in 12 specific areas of EU law; – the general limit for employers from which the employer must implement an internal notification system has been increased from 25 employees to 50; – anonymous whistleblowers enjoy the protection under the Bill only once their identity is revealed; and – determination of fines for offences under the Bill as a percentage of net turnover has been superseded by the fixed maximum fine of up to 1 Million CZK (approx. EUR 40,000). The Bill shall come into force on the first day of the second calendar month following its promulgation. Employers with 50-249 employees are required to implement an Internal Reporting System by 15 December 2023. The final version of the law is yet to be voted on by the Czech Parliament.	November 2022	Draft law (Czech)
Legal basis for indoor CCTV in hospitals	The Office for Personal Data Protection have considered whether the processing of personal data via CCTV in the indoor premises of a hospital complied with GDPR. The hospital referred to Article 6(1)(c) of GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject) and to the exception under Article 9(2)(i) of GDPR (the processing is necessary for public health reasons and serves to ensure strict quality and	October 2022	Inspection report (Czech)

Development	Summary	Date	Links
	safety standards in healthcare) to justify its processing. However, Czech law does not provide for an obligation to monitor a patients' condition using video cameras. Moreover, the inspection revealed that the CCTV footage had not been consulted in the last 10 years. The Office concluded that the hospital did not have a legal basis for the use of CCTV in the indoor premises under Article 6(1)(c) of GDPR. The Office noted though, in theory, that indoor CCTV could be operated in accordance with Article 6(1)(f) of GDPR (legitimate interest of the controller or third parties). In that case, the data controller would have to demonstrate that, for the specific purposes, the legitimate interest prevails over the rights and freedoms of the data subject.		

France

Contributors

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

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

Charlotte Haddad
Associate
charlottehaddad@
eversheds-sutherland.com

Edouard Burlet
Associate
edouardburlet@
eversheds-sutherland.com

Mélanie Dubreuil-Blanchard
Associate
melaniedubreuil-blanchard@
eversheds-sutherland.com

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

Naomi Bellaiche
Associate
naomibellaiche@
eversheds-sutherland.com

Clémence Dubois Ahlqvist
Associate
clemenceduboisahlqvist@
eversheds-sutherland.com

Killian Lefevre
Associate
killianlefevre@
eversheds-sutherland.com

Development	Summary	Date	Links
A US company (the "Company") specializing in facial recognition fined EUR 20,000,000 for several breaches of the GDPR and more specifically for unlawful processing of personal data and for failure to	The platform's facial recognition software makes use of a database of photographs and videos scraped from publicly available internet sites, including social media. The database contains over 20 billion images and fuels a search engine in which an individual's photograph can be used to attempt to identify them.	CNIL's statement: 5 December 2022 CNIL's deliberation: 17 October 2022	CNIL's statement (in English) CNIL's deliberation (in English)

Development	Summary	Date	Links
take into account the rights of individuals	A "biometric template" (i.e. a digital impression of the person's physical characteristics) is created for every individual whose image is collected by the platform. The Company offers this service to law enforcement authorities in order to identify perpetrators or victims of crime. Throughout 2020, the French Data Protection Authority (Commission National de l'Informatique et des Libertés or "**CNIL**") received several complaints relating to difficulties encountered by complainants in exercising their rights with the Company. On 26 November 2021, the CNIL issued a formal notice to the Company to comply with several provisions of the GDPR within two months. However, the Company did not provide any response to the formal notice. As a result, the restricted committee of the CNIL, in charge for issuing sanctions, issued a fine of EUR 20 million for: – Unlawful processing of personal data; – Lack of respect of individual's rights; and – Lack of cooperation with the CNIL. <u>Unlawful processing of personal data</u> The CNIL considers that the Company has no legal ground for the processing of personal data. No consent was collected from the data subjects, and the CNIL concluded that the Company was not entitled to rely on legitimate interests, since the millions of internet users whose images were collected (from social media or other websites) did not expect that their photographs or videos would be used for this purpose (especially given that the Company indicated that its software was commercialised to law enforcement agencies). <u>Lack of respect of individual's rights</u> In addition, the CNIL found that the platform: – limited the ability of data subjects to exercise their rights under the GDPR (e.g. by restricting the scope of the right of access to data collected during the previous year and by limiting the number of times per year a data subject may exercise this right); and – only provided partial responses to some requests and/or did not respond at all to requests. <u>Lack of cooperation with the CNIL</u> The Company has not responded satisfactorily to the CNIL's requests within the time limits set, and has not submitted any observations in response.		

Development	Summary	Date	Links
A voice over IP and instant messaging service company based in the US ("the Company") was fined EUR 800,000 for failing to comply with the GDPR and more specifically, on data retention periods and security of personal data	The Company is a voice over IP (technology that allows users to chat via their microphone and/or webcam over the Internet) and instant messaging social platform based in the United States. On November 17 2020, the CNIL carried out an online investigation in relation to the website and the mobile application of the Company. On the basis of the findings of its investigations, the CNIL found that the Company had failed to comply with several provisions of the GDPR, and imposed a fine of 800,000 EUR. The main areas in which the Company were found to have breached data protection laws were the following: – data retention period and information provided to data subjects; – data protection by default; – security of personal data; and – data protection impact assessments. Data retention period and information to data subject The Company has not established a data retention policy and its record of processing activities does not mention any retention period for the personal data processed. Personal data has been retained for several years, and the Company does not regularly delete nor archive personal data. Furthermore, the CNIL ruled that the information on data retention periods was not satisfactory. Data protection by default By default, the user must carry out several actions to exit the application (i.e. the application is set to remain active even when the user clicks the "X" icon at the top right of the main window). The CNIL found that this setting is misleading for the user who might think that the collection of personal data had stopped when the user clicked the "X" icon at the top right of the main window. Security of personal data When creating an account with the Company, a password of six characters including letters and numbers was sufficient. The CNIL considered that such passwords do not ensure the security of the personal data processed by the Company and does not prevent unauthorized access to user's personal data. However, the Company does now require its users to create a password of at least eight characters, with at least three of the four character types (i.e. lower case, upper case, number and special characters).	CNIL's statement: 5 December 2022 CNIL's deliberation: 10 November 2022	CNIL's statement (in English) CNIL's deliberation (in French)

Development	Summary	Date	Links
	Data Protection impact assessment The CNIL found that the Company should have carried out a data protection impact assessment since the processing activities were likely to result in a high risk to individuals' rights and freedoms given the large scale of personal data processed and the processing of minor's personal data.		
A French mobile Company was fined 300,000 EUR for failing to comply with the GDPR and more specifically on rights of individuals and security of personal data	The Company is a phone operator based in France. In 2018 and 2019, the CNIL received several complaints relating to the difficulties encountered by the complainants in exercising their rights with the Company (more specifically the right for access and deletion of their personal data). The CNIL conducted investigations which revealed several infringements of the GDPR. On the basis of the findings of the investigations, the CNIL imposed a fine of EUR 300,000. The main areas in which the Company were found to have breached data protection laws were the following: – respect of individuals' rights; and – the security of personal data. Respect of individual's rights: The Company failed to respect data subjects' right to access their data, as it did not respond to complainants in a timely manner or the responses provided were not satisfactory. The CNIL also found that the Company failed to process data subjects' erasure requests in a timely manner. Security of personal data The Company was also found in breach of the obligation to protect the security of personal data, because: – the password randomly generated by the Company when creating a user account on the Company's website, during a recovery procedure or when renewing the password, is eight characters long and can only contain one type of character; – all passwords generated when a user account was created on the Company's website were stored in clear text on the Company database; and – users' permanent passwords were transmitted by the Company by e-mail or mail, in clear text, to users when they created their account on the website.	CNIL's statement: 5 December 2022 CNIL's deliberation: 30 November 2022	CNIL's statement (in French) CNIL's deliberation (in French)

Development	Summary	Date	Links
CNIL publishes guidelines on the sale of customer databases	In December 2021, the CNIL published guidelines on the sale of customer databases. These guidelines act as a reminder to the sellers and acquirers or databases of the principles they must comply with when selling/acquiring a customer database for commercial purposes. The principles are as follows: – the database may only contain personal data of active customers. In accordance with the CNIL's recommendations, personal data used for commercial prospecting can be kept for a maximum period of three years following the end of the commercial relationship, unless an exception applies; – only data from customers who have consented or who have not objected to the transfer of their data can be marketed. The data of customers who have objected to their transmission for prospecting purposes by mail or phone call and those who have not consented to the transmission of data for prospecting purposes by electronic means shall be deleted from the database before transmission to the buyer; – the buyer must respect individuals' rights; – the buyer must inform data subjects as soon as possible, and in any event within one month (except if the information were already provided to the data subject). This information must include the origin of the data (i.e. the name of the company selling the customer database); and – the buyer must be able to prove that informed consent to commercial prospection by electronic means was obtained from data subjects.	5 December 2022	CNIL's guidelines (in French)

Germany

Contributors

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

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

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

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

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

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

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

Development	Summary	Date	Links
No special protection against termination for voluntarily hired data protection officers	On 6 October 2022, the Higher Labor Court Hamm ruled that when a company voluntarily appoints an in-house data protection officer, the special protection against termination under Sec. 6 (4) BDSG does not apply. The special protection against termination only applies if the company is legally obligated to appoint a data protection officer. In Germany, as a general rule, all companies with more than twenty employees need to appoint a data protection officer. This is a derogation to the general rules under the GDPR, where the threshold is much higher and independent of the headcount.	6 October 2022	Court decision in German

Development	Summary	Date	Links
Credit agency entry not permissible in case of disputed claim	On 28 June 2022, the District Court Frankenthal ruled that before debt collectors pass on information about non-payment of a data subject to credit agencies (e.g. Schufa), the debtors concerned must be informed in advance. If, as a result, the debtor disputes the claim, no entry may initially be made by the credit agency. If an entry is nevertheless made, the debtor can sue for revocation. Companies in this industry and companies working together with debt collectors should re-assess their processes and information notices accordingly.	Date of the decision: 28 June 2022 Date of the press release: 26 October 2022	Press release in German
Online Fonts: No claim for damage, guidance by authorities	On 20 December 2022, the District Court Munich I ruled that the use of certain online fonts violates the data protection rights of the visitors of the websites on which the fonts are implemented, if implemented in a dynamic way. In this case, by way of dynamic implementation, IP addresses of the users were transferred to US servers, which requires a valid consent. However, valid consent is not always requested from the user. As a result, there has been a wave of warning letters against website operators who use online fonts. The State Officer for Data Protection of Lower Saxony recommends downloading the fonts and saving them locally on the server to avoid the data privacy violations. In addition, the judiciary is now investigating one of the lawyers sending the warning letters on behalf of his client, for commercial fraud and extortion. Companies are recommended not to pay the "settlement amount" as requested by the lawyer. Lastly, the local court Charlottenburg (217 C 64/22) ruled that the data subject has no entitlement to claim for damages as no damage was proven by the claimant and overall, the facts underlying the claim were too generic.	Date of guidance: 6 October 2022 Date of Decision: 20 December 2022	Statement in German Court Decision in German
No compensation as a result of data scraping in the case of data made openly accessible on the Internet	A third party had copied and collected personal data which the plaintiff had posted publicly on a social media platform (so called "**data scraping**"). As a result, the plaintiff sued the operator of the social media network for compensation for pain and suffering, based on the "inner turmoil" caused. The District Court Giessen has ruled that such damages for pain and suffering cannot be claimed if the personal data concerned is voluntarily posted publicly for everyone to access.	3 November 2022	Court decision in German
DSK guidance on cookies et al.	The Independent Federal and state Data Protection Authorities ("**DSK**") has published a new version of its Telemedia Guideline, which includes guidance and interpretationin particularly in relation to the use of cookies. The updated guidance is the result of a comprehensive consultation phase, where the public had an opportunity to comment on the initial draft. The assessment of the consultation phase addressed various points issued by the public, including the determination of telemedia services	5 December 2022	Updated guidance by DSK Assessment of consultation by DSK in German

Development	Summary	Date	Links
	explicitly requested by the user (i.e. the differentiation of basic and additional functions, which is decisive in respect of the need for consent). The guidance also addresses the interpretation of "absolutely required" and a "decline button" at the first level. In light of this new Guideline, companies should assess their website and app structure and draw specific attention to the cookie consent mechanism.		

Hong Kong

Contributors

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

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

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

Kelvin Ng
Trainee Solicitor
KelvinNg@
eversheds-sutherland.com

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

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

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

Karen Fan
Trainee Solicitor
KarenFan@
eversheds-sutherland.com

Development	Summary	Date	Links
PCPD publishes investigation report on EC Healthcare's sharing of clients' personal data among its various brands through an integrated system	The Office of the Privacy Commissioner for Personal Data ("**PCPD**") published its investigation report on EC Healthcare, a company listed on the Hong Kong Stock Exchange which provides one-stop medical and health management services. The investigation arose from two complaints lodged with PCPD regarding the sharing of clients' personal data among several brands within the EC Healthcare group through an integrated internal system (the "**System**"). By way of background, the two brands relevant to the complaints were independent organisations acquired by EC Healthcare. Following the	14 November 2022	Media Statement Investigation Report

Development	Summary	Date	Links
	acquisitions, the existing clients of the acquired brands were automatically made members of EC Healthcare and their personal data was stored in the System. The PCPD has found that EC Healthcare contravened the requirements of Data Protection Principle 3(1) on the use (including disclosure and transfer) of personal data as follows: – the personal data originally provided by the complainants to a single brand and was disclosed and transferred, without their knowledge, to the staff of some other brands. This arrangement was inconsistent with the original purpose of collection of personal data and fell short of their reasonable expectation for personal data privacy; and – after the acquisitions, EC Healthcare failed to obtain consents from the existing clients of the acquired brands for the use, disclosure and transfer of their personal data among various brands within the EC Healthcare group. EC Healthcare also failed to inform such clients that their personal data would be stored in the System. As a result, the PCPD served an Enforcement Notice on EC Healthcare pursuant to section 50(1) of the Personal Data (Privacy) Ordinance (the "**PDPO**"), which directed EC Healthcare to take remedial actions to remedy and prevent recurrence of the relevant contraventions.		
PCPD publishes investigation report on ransomware attack on Fotomax's database	In October 2021, Fotomax notified the Office of the Privacy Commissioner for Personal Data ("**PCPD**") that its online store database had been attacked by ransomware and maliciously encrypted. Approximately 545,000 members and 74,000 customers were affected. Prior to the incident, Fotomax had in place a firewall supplied by a third party provider and also enabled Secure Sockets Layer Virtual Private Network (the "**SSL VPN**") to allow remote access to Fotomax's system. Subsequently, the firewall manufacturer issued a security advisory of a vulnerability in its firewall solution where SSL VPN is enabled. It urged users to disable the SSL VPN and to implement multi-factor authentication. This was followed by a high threat security alert issued by the Hong Kong Government Computer Emergency Response Team on the said vulnerability. At the time, Fotomax considered it unnecessary to immediately patch the vulnerability on the basis that it had anti-virus software, anti-ransomware programme and firewall in place and that the SSL VPN was only used by its IT department. Fotomax did not re-evaluate this position when the SSL VPN was leveraged for work-from-home arrangements due to the COVID-19 pandemic.	14 November 2022	Media Statement Investigation Report

Development	Summary	Date	Links
	The PCPD has found that there were serious deficiencies in Fotomax's risk awareness and personal data security measures implemented. In particular, Fotomax had: – misevaluated the risk of the security vulnerability and failed to take sufficient action for system security; – failed to properly manage the information system which contained personal data, such as not having a robust patch management program; and – failed to implement multi-factor authentication as recommended by the firewall manufacturer to prevent cyberattacks. As a result, the PCPD considered that Fotomax contravened the requirements of Data Protection Principle 4(1) concerning the security of personal data. The PCPD served an Enforcement Notice on Fotomax pursuant to section 50(1) of the PDPO, which directed Fotomax to take remedial actions to remedy and prevent recurrence of the relevant contraventions.		
Hong Kong Court hands down first conviction for doxxing	The Hong Kong Court handed down the first conviction for a doxxing offence under the Personal Data (Privacy) Ordinance ("**PDPO**") since the new anti-doxxing regime took effect in October 2021. Between 19 and 26 October 2021, the defendant, a 27-year-old male set up fake profiles on social media platforms to impersonate his former girlfriend and invited the public to visit her home. In the course of creating those profiles, he disclosed on four social media platforms his former girlfriend's personal data, including her name, photos, residential address, telephone numbers, name of her employer and job title. This led to strangers approaching her in the hope of becoming acquainted with her. The defendant was arrested in June 2022. Two months later, sevencharges were laid against him under the PDPO. Under section 64 of the PDPO, it is unlawful for anyone to disclose any personal data of a data subject without consent from the data subject if he/she is equipped with an intent to cause any harm to the data subject or the data subject's family member, or is reckless as to whether any specific harm would be caused. "Harm" is defined broadly under the law to include any harassment, molestation, bodily and psychological harm. The defendant pleaded guilty to and was convicted of all seven charges. The Court considered the need for deterrence and handed down a sentence of eight months' imprisonment.	15 December 2022	Media Statement

Hungary

Contributors

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

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

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

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

Development	Summary	Date	Links
Authority's statement in response to a journalist's inquiry about a change in the ownership of a free online mail system	The Hungarian National Authority for Data Protection and Freedom of Information ("**NAIH**") has made a statement in response to a journalist's inquiry about a change in the ownership of a free online mail system, particularly in relation to the obligation to provide information to data subjects in connection with changes in the identity of the controller as a result of a merger. New Wave Media Group Kommunikációs és Szolgáltató Korlátolt Felelősségű Társaság ("**Freemail**") recently merged into Mediaworks Hungary Zrt ("**Mediaworks**"). The NAIH confirmed through its statement that in the case of a merger of a business entity into another entity, the merging legal entity ceases to exist and is succeeded by the other legal entity participating in the merger. Accordingly, on the day of the merger, the rights and obligations of the merging company transferred to the acquiring company by operation of law, including the contracts and the related data processing. As Mediaworks became the legal successor to Freemail, the NAIH is of the view that the personal data processed must be considered to have been obtained by Mediaworks (through its predecessor) directly from the data subjects, and Article 13 of the GDPR must be applied accordingly. Recital 61 of the GDPR helps to interpret the obligation to provide information. "Information relating to the processing of personal data concerning the data subject shall be provided to the data subject at the time of collection or, where the data has been collected from another source than the data subject, within a reasonable period, having regard to the circumstances of the case". However, the GDPR does not provide for specific rules on the provision of information in cases where there is a	15 December 2022	Authority statement in Hungarian

Development	Summary	Date	Links
	change, for whatever reason, in the information previously provided by the controller. The NAIH has assumed that Freemail provided information to data subjects at the time of collection of the data in accordance with Article 13 of the GDPR, so that its successor was only required to provide information on new information relating to any changes to the processing. Whether the information required by the GDPR was provided to data subjects by a controller at the appropriate time and whether the data subjects' rights to the protection of personal data was infringed can only be determined by the NAIH in its specific proceedings, taking into account all the circumstances of the case.		

Ireland

Contributors

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

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

Ellie Cater
Senior Associate
T: +35 31 66 44 28 0
elliecater@
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
The DPC publishes One-Stop-Shop Cross-Border Complaints Statistics Report	The Irish Data Protection Commission ("**DPC**") has published an update to its March 2022 report which contained a statistical overview and analysis of the DPC's handling of One-Stop-Shop ("**OSS**") complaints. The latest report outlines the cross-border complaint handling processes employed by the DPC along with information regarding the volume of complaints received, the amount concluded, and the outcomes of various complaints. Since the GDPR came into force, the DPC has received nearly 20,000 complaints of which over 17,000 have since been concluded.	26 January 2023	DPC Report
The DPC publishes updated guidance for data controllers regarding subject access requests	The DPC has updated its guidance for data controllers regarding data subject access requests. The guidance has been drafted to assist data controllers in identifying the primary practical issues of compliance with data protection legislation in respect of access requests.	1 October 2022	DPC Guidance
The DPC submits Article 60 draft decision on inquiry into a social media company	The DPC has submitted a draft decision in a significant inquiry into a social media company to various data protection authorities across the EU. The inquiry relates to the publication of a dataset of approximately 553 million user's personal data on the internet. The inquiry is concerned with	3 October 2022	See DPC note here.

Development	Summary	Date	Links
	the social media company's compliance with Articles 25(1) and 25(2) of the GDPR ("data protection by design and by default").		
The DPC submits Article 60 draft decision on inquiry into web services provider	The DPC has submitted a draft decision in an inquiry into a web search engine/services provider (the "**Company**") to Data Protection Authorities in the EU. The inquiry was initiated in August 2019 and involved the Company's compliance under Articles 5(1)(a), 12, 13 and 14 of the GDPR, which concern the processing of personal data. In particular the inquiry investigated compliance with transparency of information to data subjects.	7 November 2022	DPC Note
The DPC decision in "Data Scraping" Inquiry	The DPC has completed an inquiry into a social media company and has applied a €265 million fine along with a number of corrective actions. The inquiry concerned an investigation and determination of social media tools in relation to the processing of data carried out from 25 May 2018 to September 2019. The primary issues centred around compliance with the "Data Protection by Design and Default" obligation under the GDPR.	28 November 2022	See DPC note here.
Statutory Instruments no. 601, 602 and 603 of 2022 are signed into law	The Irish Government has signed into law three statutory instruments ("**SIs**") regarding the processing of personal data by the Irish Auditing and Accounting Supervisory Authority ("**IAASA**"), the Corporate Enforcement Authority ("**CEA**") and the Competition and Consumer Protection Commission ("**CCPC**"). The purpose of the SIs is to provide for the restriction of certain rights and obligations under the GDPR. Such restrictions may apply to certain processing carried out by the IAASA, CEA and CCPC in the pursuit of their relevant objectives. The SIs contain the prescribed limited circumstances as to when such restrictions may be applied.	28 November 2022	SI 601 SI 602 SI 603
DPC fines confirmed	The DPC had its decisions to implement administrative fines affirmed in the Circuit Court in respect of six entities with the fines varying from EUR 1,500 to 17 million.	30 November 2022	DPC Note
DPC welcomes latest successful prosecution of Marketing Offences	The DPC has welcomed the successful prosecution of a publishing company, Guerin Media Limited in relation to the sending of unsolicited marketing communications without consent. The Court imposed a total fine of EUR 6,000. The DPC has noted that "the outcome of these proceedings should serve as a reminder to all organisations that are engaged in any form of electronic marketing, such as by email, text message or cold calling, that non-compliance with the	5 December 2022	DPC Note

Development	Summary	Date	Links
	regulations may result in a criminal prosecution by the Data Protection Commission."		
S.I. No. 137/2022 - Data Sharing and Governance Act 2019 (Commencement of Certain Provisions) Order 2022	From 16 December 2022 sections 6(2) and 6(3) of the Data Sharing and Governance Act 2019 have come into operation. Section 6(2) of the Data Sharing and Governance Act provides that section 38 of the Data Protection Act 2018, which provides a legal basis for processing a task carried out in the public interest or in the exercise of official authority, shall not apply to the disclosure of information by one public body to another public body.	16 December 2022	SI
The Data Protection Commission launches inquiry into a social media company	The DPC has begun an inquiry following media reports stating that collated datasets of users' personal data from a social media company have been published on the internet. Reportedly the datasets contain personal data concerning approximately 5.4 million users worldwide and map users' IDs to email addresses and/or telephone numbers of the applicable data subjects. The DPC is currently assessing whether GDPR obligations have been breached following information being submitted to the DPC from the company.	23 December 2022	See DPC note here.

Netherlands

Contributors

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

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

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

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

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

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

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

Development	Summary	Date	Links
Outlines of DDPA's algorithm supervision	Alexandra van Huffelen, Minister for Digitisation, has informed the House of Representatives on the algorithm supervision to be set up as part of the Dutch Data Protection Authority ("**DDPA**"). The letter to parliament states which new activities the DDPA, together with the other boards, market regulators and state inspectorates, will be working on in 2023. In addition, the existing supervision of algorithms that (unlawfully) process personal data will be strengthened in 2023. Algorithms can have a major impact on human lives and society. With the algorithm supervision at the DDPA, Van Huffelen is fulfilling the ambition	22 December 2022	Outlines of DDPA algorithm supervision (Dutch only)

Development	Summary	Date	Links
	of the House of Representatives and the Dutch government to ensure that algorithms are checked for transparency, discrimination, and randomness. An important part of the new supervision is identifying and analysing cross-sector and domain-transcending risks of algorithms, and facilitating and intensifying cooperation with other organisations. With this new task, the DDPA will specifically focus on risks that transcend sectors and domains. Existing powers and duties of other boards, market regulators and state inspectorates are not subject to change. Strengthening cooperation between these authorities is important in this respect, so that risks of discrimination, exclusion, and lack of transparency can be identified and tackled more quickly through shared knowledge and insights. The DDPA started these new activities at the beginning of January 2023. During the initial period, the focus will be on identifying risky algorithms, pooling knowledge, and further shaping collaboration.		
Dutch police fined for missing risk analysis for the use of camera cars in Rotterdam	The DDPA fined the Dutch police €50,000 due to a missing risk analysis (DPIA) for the use of camera cars in the city of Rotterdam. During COVID-19, camera cars were deployed in Rotterdam without assessing any privacy risks. Detailed images of individuals were collected and stored through use of the moving cars. The DDPA's investigation also concluded that too many images were taken, which was deemed unnecessary. In 2020, the municipality of Rotterdam and the police deployed two cars equipped with 360-degree cameras for five weeks. Through the use of the cars, the municipality and police wanted to check whether people kept a distance of 1.5 meters from each other due to social distancing requirements during COVID-19. Even at a speed of 50 kilometers per hour, the cameras could capture sharp images with enough detail to identify individuals. Far beyond the initial radius of the camera cars, individuals were recognisably captured on camera. The images collected were viewed in a control room, stored and could be forwarded to other police locations. The police are legally responsible for the images as police data. In May 2020, the DDPA sought clarification on the use of the camera cars, after which the use was temporarily suspended. After receiving signals that the camera cars were in use again, the DDPA launched an investigation. The DDPA now concludes that the law was breached in two ways. In addition, the DDPA found that there are different views on the lawful basis for the deployment of camera cars. Prior to taking the camera footage, the police did not analyse the potential privacy risks in a data protection impact assessment ("**DPIA**"). A DPIA was necessary because the police could have known that the	21 December 2022	DDPA Fine (Dutch only)

Development	Summary	Date	Links
	deployment of the camera cars was likely to pose a high privacy risk towards individuals. Moreover, the police would collect personal data from large groups of people in public, who are unlikely to know that images are being collected or how they are being used. This is a violation of the Police Data Act ("**PDA**"), which contains the main privacy laws for the police in the Netherlands. In conclusion, too many images were collected and stored that were not necessary for carrying out police work. The police acknowledged this violation of the PDA. Whilst the DDPA monitors compliance with the PDA, it cannot impose a fine for a violation under the PDA. The police still have the possibility to object to the DDPA's fine.		
DDPA objects to proposal on the regulation of staffing and temporary staff agencies	The DDPA has objected to a proposal from the Dutch government in relation to regulation of the market for outsourcing staff. Under the proposal, staffing and temporary employment agencies will only be allowed to offer temporary workers if the agencies have a special certificate showing that they meet certain standards. The proposal also concerns companies and institutions that hire temporary staff, such as companies in construction, healthcare, horticulture or hospitality. Hirers may only hire staff from staffing and temporary employment agencies if they have obtained the special certificate. To check whether hirers comply with this rule, they can be audited. It is unclear whether the hirers have to provide personal data and, if so, which type of data. For example, it is not clear whether hirers have to provide data of individual workers. The DDPA concludes that the role of personal data in the system is very unclear. The proposal mentions that the exchange of personal data is necessary, but hardly explains what personal data is involved, or who should provide data to whom and why. The DDPA has its doubts as to whether the data processing is necessary for the certification systems at all, as it currently lacks restrictions, transparency and motivation. The certificates will be issued by a new body, which is yet to be established. Accordingly, the newly established body will appoint monitoring bodies to oversee compliance.	20 December 2022	DDPA Statement (Dutch only)
The DDPA limits the use of personal data of mental healthcare patients by the Dutch Healthcare Authority (NZa)	The DDPA limits the use of personal data of mental healthcare patients by the Dutch Healthcare Authority ("**NZa**"). The NZa wants to require mental healthcare providers to provide information about their patients. The information would be used to calculate healthcare costs more accurately, something which the NZa is legally authorised to do. The DDPA now sets strict conditions for the implementation of this proposal. Data about	14 December 2022	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	(mental) health is very sensitive in nature and as such, health data is additionally protected under the GDPR. The NZa explicitly states that it will not receive any data that is directly traceable to individual patients. Further, the generalised information it receives is not linked to files with which the information could still be traced back to individual persons. In addition, the DDPA prescribes strict conditions. For example, the NZa may only request data from all mental healthcare patients over a period of one year on the basis of the Mental Healthcare and Forensic Care Regulations. If the NZa would need the data for the new system at a later time, it must first develop a new statutory regulation with a substantiation for that particular need. Moreover, the new Regulation must first be submitted to the DDPA, so that it can assess whether the Regulation is lawful and whether the privacy of patients is guaranteed. The NZa guarantees that it will only use the requested data for the development of the new system in mental healthcare. The DDPA indicates that the NZa must record this in writing within a new version of the Mental Healthcare and Forensic Care Regulations.		
Suspicion of algorithmic discrimination has been successfully substantiated before The Netherlands Institute for Human Rights	A student has succeeded in providing sufficient facts for a suspicion of algorithmic discrimination. The claimant argued that the "Vrije Universiteit" – a Dutch University - discriminated against her through the use of anti-cheating software. This software uses face detection algorithms. The software did not detect the claimant when she had to log in for her exams. The claimant suspected that this was due to her skin colour. The University has been given ten weeks by the Executive Board to demonstrate that the software does not discriminate against individuals based on their race.	9 December 2022	Intermediate Judgment - Institute for Human Rights (Dutch only)
Legislative proposal submitted to update Dutch GDPR Implementation Act	According to the Dutch government, the Dutch GDPR Implementation Act ("**UAVG**") and a number of other laws should soon be amended, addressing 16 different subjects. The Dutch GDPR Implementation Act lacks necessary clarification on certain points, such as outdated references, and the Court has ruled against the purpose of a single provision. Various points for improvement have been brought forward in the past 5 years since the law has been in force. Changes are also being proposed for the Aliens Act, the Road Traffic Act and the Financial Supervision Act, for example, in order to better align them with the GDPR and the UAVG. Advice has been obtained from, among others, employers' organisations, the Association of Dutch Municipalities (VNG) and the DDPA.	6 December 2022	Proposal amendments of Dutch GDPR Implementation Act (Dutch only)

Development	Summary	Date	Links
	The adjustments include the following: – More rights for children between the ages of 12 and 16; – Less broad interpretation of the concept of criminal personal data; – Making it more simple for accountants to process sensitive personal data; – Amendments to simplify the work of trustees; – Clarification that biometric data may only be used for the purpose of access to certain places, services, information systems, etc.; and – In the situation of a care provider retiring or passing away, the transfer of files of their patients to another care provider, who keeps them during the legal retention period, will be better regulated.		
The Dutch government will not interfere with the DDPA's decision regarding the Dutch Tennis Association's (KNLTB) fine	The Dutch government does not intend to enter into discussions with the DDPA regarding the fine imposed on the Royal Dutch Lawn Tennis Association ("**KNLTB**") in early 2020. In March 2020, the DDPA imposed a fine of €525,000 to the KNLTB. The tennis association sold personal data to sponsors for personalised advertising. The data was sold without informing the data subjects and without permission. The KNLTB argued there was a legitimate interest. By selling members' personal data to sponsors, the tennis association strengthened its economic position. The DDPA stated that a commercial interest can never be a legitimate interest. During summer 2021, the European Commission warned the Dutch regulator that with this position it interpreted the GDPR too strictly, which is not good for the functioning of the internal market and freedom to conduct business. Regardless, the DDPA felt justified in its decision. The DDPA emphasised that regulators have an independent position, also stating that the interpretation of the DDPA does not conflict with rulings of the Court of Justice of the European Union. The House of Representatives raised parliamentary questions on whether the Minister for Legal Protection should enter into consultations with the DDPA with the request to reverse the fine. The Minister for Legal Protection emphasises that the independence of the supervisor is laid down in Article 52 GDPR. According to the Minister, this also applies to legal proceedings. In addition, the national government is not a party to the conflict and should not interfere in legal proceedings. The Minister sees no reason to launch an investigation into the actions of the regulator.	5 December 2022	Parliamentary questions House of Representatives (Dutch only)

Netherlands

Development	Summary	Date	Links
Court ruling on GDPR violation of a request for access and erasure of personal data by Dutch insurance company	The dispute in this case was between applicant and ASR (a Dutch insurance company) on whether ASR has complied with its GDPR obligations. Following a data subject access request by the applicant, ASR provided an overview of the applicant's personal data. The applicant was of the opinion that the overview provided was incorrect and incomplete. The applicant argued that ASR acted in violation of the GDPR. The Court ruled that ASR's conduct was unlawful. This is due to ASR wrongly disclosing the applicant's email address and policy number to his ex-partner, without the applicant's consent. ASR has stated in an exhibit accompanying the statement of response that the applicant has "severe rheumatism". This concerns a special category of personal data of the applicant that may not be processed. Nevertheless, the claims for damages were rejected. The claim for nonpecuniary damages was rejected because the applicant had not fulfilled his obligation to furnish facts. The pecuniary damages were also rejected because there was no causal connection.	25 November 2022	Court Decision (Dutch only)
Dutch UBO register no longer public following ruling by the CJEU	The CJEU declared the provision of the Fifth Anti-Money Laundering Directive invalid. The Directive obliges EU Member States to ensure that the information regarding Ultimate Beneficiary Owners ("**UBO**") of companies and other legal entities incorporated within their territory are accessible to all members of the public. According to the Court, this access constitutes a serious interference with the fundamental rights to respect for private life and the protection of personal data as laid down in the Charter of Fundamental Rights of the European Union. The Court ruled that this interference is not limited to what is strictly necessary and is not proportionate to the aim pursued. In the Netherlands, as a result of this ruling, Finance Minister Kaag instructed the Chamber of Commerce not to provide any information from the UBO register for the time being. In a letter to House of Representatives, the Minister promised to study the Court's judgment in the upcoming period and to consult with the European Commission on which information can be released. Until such consultation has taken place, the Minister has indicated that the registration obligation for UBOs in the Netherlands will in any case continue to exist.	22 November 2022	Letter to Dutch Parliament (Dutch only)
The DDPA advises that the Dutch government must tackle the privacy risks of the new cloud policy	The Dutch government wants to be able to store government data in commercial cloud services going forwards. According to the DDPA, this entails major privacy risks, which the government must address in further elaboration of its policy.	14 November 2022	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	At the end of August 2022, the State Secretary presented a new cloud policy. The policy has the aim to enable government agencies to use commercial cloud services. In this way, the government would be allowed to store personal information concerning Dutch citizens on servers of, for example, US based cloud providers. Currently, storage with such commercial cloud providers is not permitted. When selecting cloud providers - located in countries where the level of protection of personal data is not equivalent to the EU - the government must properly identify the risks in advance and take measures to ensure that the data is sufficiently protected. The DDPA advises that storage with a European cloud provider is currently preferable for ensuring privacy.		
Court of Amsterdam rules that Dutch Court has jurisdiction to adjudicate claims by Dutch foundations against international social network	Three Dutch foundations intend to commence legal proceedings against an international social network in the Netherlands. They claim a total of approximately €9.4 billion in damages from the social network, due to violations of the privacy of Dutch users in connection with violations under the Telecommunications Act and the Media Act. The Court of Amsterdam has now ruled that the Dutch Court is competent to deal with the substance of the dispute. The substantive hearing will take place in February 2023. The social network has argued that the Dutch Court does not have jurisdiction to hear the claims of the foundations, since its EU establishment is in Ireland, the Irish Court should be deemed competent instead. The social network also wants to await an investigation by the Irish regulator, the Data Protection Commission, as well as seek advice from the CJEU.	9 November 2022	Court Decision (Dutch only)
DDPA warns that the new draft legislative proposal 'Plan of action money laundering' will lead to unprecedented mass surveillance by banks	The draft proposal for the new law on anti-money laundering formulates a number of principles: – A ban on cash payments for goods costing more than €3,000. – The possibility for banks to jointly monitor their clients' transactions. – The obligation to exchange specific risks between the banks. Part of the proposal is to monitor all bank transactions of all Dutch account holders in one centralised database, using algorithms. In the DDPA's opinion, this represents a far-reaching breach of the protection and confidentiality of customer data. Banks are already required to carry out individual checks on people or companies that may be laundering money or financing terrorism. They must report unusual transactions to the authorities.	21 October 2022	DDPA Statement (Dutch only)

Development	Summary	Date	Links
	The proposal gives banks powers that go even further. Based on the proposal, banks will be able to collect and monitor the payment behaviour of all Dutch citizens in one common place. Banks plan to quickly outsource the monitoring to a third party that uses algorithms. In addition, banks will be able to start exchanging customer data with each other. The risks entailed by this system are disproportionate to the purpose of the draft proposal. For example, this would be a substantial risk to the rights and freedoms of account holders. If account holders are wrongly designated as a high risk by one bank, then this would have the consequence of a negative registration against their name at all other banks in the Netherlands. It could become practically impossible for such citizens to obtain a bank account anywhere in the country. The Council of State, the government's highest advisory body, also indicated in an earlier advisory report the customer privacy issues at stake. Shared transaction monitoring and data exchange could lead to discrimination and exclusion.		
The Dutch government presents the Dutch cybersecurity strategy (NLCS) 2022-2028	According to the Minister of Justice and Security, the digital threat is rapidly increasing and immediate action is necessary to increase organisations' digital resilience, strengthen systems and tackle the threat. Only then will the Netherlands be able to safely capitalise on the economic and social opportunities of digitalisation, while at the same time protecting its security and public values. The Netherlands is one of the most digitised countries in the world. The Dutch government emphasises the need to protect these systems and make sure the Netherlands is prepared in case of any cybersecurity threats. Concrete actions for a digitally secure society are included in the strategy plan 2022-2028. To realise the vision, goals have been formulated in line with four pillars: – Increasing the digital resilience of the government, companies and civil society organisations; – Offering safe and innovative digital products and services across the country; – Countering digital threats from other states and criminals; and – Sufficient cyber security specialists, education about digital security and digital resilience of citizens. To achieve these goals, the system for digital security will be strengthened. To this end, for example, the National Cybersecurity Center, Digital Trust Center and the Cyber Security Incident Response	10 October 2022	Publication Dutch Cybersecurity Strategy (Dutch only)

Development	Summary	Date	Links
	Team for Digital Service Providers will be merged into one national cybersecurity authority. The strategy was developed with the broad involvement of many public, private and civil society organizations and builds on previous government-wide cybersecurity strategies from 2011, 2013 and 2018. All Ministries are working together on the development and implementation of the strategy, including with public and private partners.		
Evaluations of individual accountants may not be published outright	The Dutch government intends to publish assessments of the work of individual accountants. The DDPA finds that this is an excessive breach of the privacy of accountants. They advise the Dutch government to amend their draft legislative proposal. On May 10 2022, the DDPA issued critical advice on the proposed Future Accountancy Sector Act to Minister Kaag of Finance. The proposal was amended accordingly. After reviewing the amended proposal, the DDPA concludes that it still does not safeguard the privacy of accountants in a sufficient manner. The government is of the opinion that the quality of the accountancy sector is under pressure and explains why the quality of the supervision of this sector should be improved. One of the Commission's recommendations for the future of the accounting industry is to require certain accounting firms to report their performance periodically to the authorities drawn from the profession. Publishing reports of an accountant's performance including names is considered an invasion of that accountant's privacy. It can have major consequences for an accountant's reputation and career. A negative review can mean that someone may experience difficulty to acquire work. If an accountant's individual performance is to be published, it is essential that there are sufficient safeguards. Such safeguards include the ability to defend against an unjustified assessment and that there are clear limits to the data processing. A substantial breach of a person's privacy as proposed by the government is not allowed without cause. Any such publishing should only be allowed if there are no other less intrusive options possible. The DDPA finds the proposal insufficiently concrete on the abovementioned points.	4 October 2022	DDPA Recommendation (Dutch only)
The District Court of Zeeland-West-Brabant rules that refusal of online camera surveillance is not a	The District Court ruled that a Dutch employee employed by a US employer was unfairly dismissed after refusing to turn on his camera during the entire working day.	4 October 2022	Court Decision (Dutch only)

Development	Summary	Date	Links
ground for dismissal of an employee	The applicant had joined the employer, Chetu Inc., in January 2019. On 23 August 2022, the applicant received an e-mail from the employer informing him that he had to immediately participate in the Corrective Action Program - Virtual Classroom. In addition, he had to be logged in throughout the working day, share his screen and leave his camera on. The applicant objected to having his camera on for 9 hours a day whereby his employer could monitor all his activities through his screen. On 26 August 2022, after the employer had sent two insisting and intrusive instructions to the applicant to turn on his camera, the applicant received an email stating the employment was terminated due to refusal of work and insubordination. The District Court ruled that leaving the applicant's camera on for full working days violates his right to respect for his private life and the employer had no justifiable reasons to do so. The Court found that the employer had no urgent cause for termination of the employment relationship. The Court ordered the employer to pay the applicant approximately €80,000 in compensation and damages.		

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: data controller must comply with the procedures it has implemented	The Polish Data Protection Authority ("**DPA**") imposed an administrative fine on the mayor of the Dobrzyniewo Duże commune in the amount of PLN 8,000. The breach consisted of the theft of an employee's computer which held personal data, on which appropriate safeguards were not applied to protect the data, resulting in a breach of confidentiality. The theft occurred off the controller's premises as the employee using the laptop was storing it at home. Prior to the breach, the controller had developed appropriate procedures and policies for the security of personal data processing and conducted a risk analysis that addressed, among other things, the threat of the theft of computer equipment used to process personal data. As the proceedings showed, the stolen computer was protected from unauthorised access only by a password, and the security measures adopted in the controller's internal procedures were not applied, at least on this device. Only after the breach did the controller take measures to avoid similar occurrences in the future by encrypting laptops' hard drives and following the results of its own risk analysis and the risk management measures set out therein.	16 November 2022	DPA announcement (in Polish)

Development	Summary	Date	Links
	The controller was negligent resulting in the occurrence of a data confidentiality breach, thereby inadvertently violating data protection regulations.		
Polish Supreme Administrative Court: license plates do not constitute personal data - III OSK 1522/21	The Polish Supreme Administrative Court ("**SAC**") ruled that license plates do not constitute personal data. The judgment relates to a footage from the police video recorder. A citizen demanded that the police release it as public information. The police released only parts of it, concluding that releasing the whole video could result in a breach of privacy. The reason was that the four people under inspection were recorded, as well as the license plates of the vehicles. The Voivodship Administrative Court in Szczecin dismissed the complaint against the decision, finding the police's reasoning to be correct. The Court recognised that it is possible to determine the personal data of the vehicle's owner if someone has the license plate number, make and color of the vehicle. This could easily be obtained for example, by posting a photo on a social media site. It does not matter whether a specific person can be identified, directly or indirectly, and this can consequently lead to a breach of their privacy. The SAC disagreed with this approach. It cited previous judgments in similar cases and accepted that license plates do not contain personal data. The SAC shared the view expressed in an earlier judgment of May 14, 2021 (Case No. III OSK 1466/21), according to which "a car's license plate number does not fall under the protection of the right to privacy, as it identifies the car, not the person." In its justification, the SAC referred also to Article 4(1) of the GDPR and stated: "Personal data thus constitutes information concerning natural persons, with such information making it possible to determine the identity of such person directly or with the use of simple identification tools in the possession of the entity that wants to obtain or process such data. Thus, if the definition of personal data refers to natural persons - data on a thing (a car) does not constitute information referred to in Article 4(1) of the GDPR, if the identification of the holder of that thing can only be done by accessing the relevant registers or catalogs." It is worth noting that this judgment has been criticised in Poland and other European authorities express a different position than the one presented by the Polish SAC.	3 November 2022	Judgment (in Polish)

Poland

Development	Summary	Date	Links
The Polish Data Protection Authority: a controller must regularly test, measure and evaluate the effectiveness of the technical and organizational measures adopted to ensure the security of processing	The Polish Data Protection Authority ("**DPA**") decided to impose an administrative fine of almost PLN 1.6 million on a telecommunication company. The breach of the protection of subscribers' personal data occurred as a result of exploiting a vulnerability in the IT system. According to the DPA, the lack of procedures for regularly testing, measuring and evaluating the effectiveness of the technical and organisational measures adopted to ensure processing security contributed to the personal data breach. Such measures were taken only after the breach occurred in December 2019. In practice, the penalty assumes a position as if the controller had not taken such measures at all. Significantly in this case, the last comprehensive review of technical and organisational measures by the company was carried out in May 2018 - when the GDPR began to apply. The company, despite the solutions adopted, was unable to detect vulnerabilities due to the lack of regular testing. Performing reviews once or when an organisational or legal change occurs, as well as taking action only when a vulnerability is suspected, cannot be considered regular testing, measuring and evaluating the effectiveness of the technical and organisational measures in place. After investigating the case, the DPA found that the company had not properly implemented the requirements of the GDPR, which led to a breach in the protection of subscribers' personal data.	9 December 2022	DPA Announcement (in Polish)
Poland's first GDPR-compliant Code of Conduct approved by DPA	The Polish Data Protection Authority ("**DPA**") approved the Code of Conduct regarding the protection of personal data processed in small medical facilities. The purpose of the Code of Conduct is to ensure the protection of the personal data of patients and others in healthcare facilities. The adopted Code of Conduct will not only help medical entities comply with the requirements of GDPR, but also spread awareness of data protection among patients. Entities that will apply it can have a guarantee of the correctness of the use of certain solutions approved by the DPA. They can also count on supervision of personal data processing processes by an independent entity monitoring the Code. It is significant that under the GDPR, the DPA when considering imposing a penalty on an entity, must consider in each case whether the entity is correctly applying the approved Code of Conduct.	14 December 2022	DPA Announcement (in Polish)

Development	Summary	Date	Links
	This is the first such Code of Conduct approved in Poland.		
Voivodship Administrative Court: telephone number alone does not constitute personal data	The Polish Voivodship Administrative Court ("**VAC**") ruled that a telephone number alone does not constitute personal data. The latest judgment concerns a phone numbers database. It was created by a telemarketing company that obtains phone numbers from the Internet. Its employees called the numbers and asked if the subscriber was interested in obtaining information about English courses. If they were, the company asked for data such as name and consent to the processing of personal data for marketing purposes. If not, the company put the number on an internal "blacklist" so that they would not call it again. The VAC stated that telephone numbers alone (without other subscriber information) are not, or at least do not have to be, personal data. The VAC recognised that personal data is information about an identifiable person, not information that makes it possible to verify the identity of an individual. From the views of the doctrine and the jurisprudence of the administrative courts, it follows that a telephone number may constitute personal data in a situation where the disposer of that number is also in possession of other information that makes it possible to identify, such as a name or address. According to the VAC, the Polish Data Protection Authority ("**DPA**") cannot assume in advance that processing is taking place. The court found the allegations of the complaint accurate, according to which the DPA erred in determining that the processing of personal data occurs when only the phone number is in its possession.	25 November 2022	Judgment (in Polish)

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
Amendments to the Enforcement Regime under the Personal Data Protection Act 2012	The Personal Data Protection Commission of Singapore ("**PDPC**") has updated its Advisory Guidelines on Enforcement of the Data Protection Provisions ("**Advisory Guidelines**") to reflect various amendments to the enforcement regime under the Personal Data Protection Act 2012 of Singapore ("**PDPA**"). The key amendments to the Advisory Guidelines are as follows: – The PDPC is allowed to accept voluntary undertakings as part of the enforcement regime; – Increase in the maximum financial penalties which the PDPC may impose for intentional or negligent breaches of the PDPA: – breaches of the data protection provisions: S$1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher; and – breaches of the 'Do Not Call' provisions involving the use of dictionary attack and address-harvesting software: S$200,000 for individuals, 5% of a person's annual turnover in Singapore where such turnover exceeds S$20 million, and S$1 million in any other case.	1 October 2022	PDPC's Advisory Guidelines on Enforcement of the Data Protection Provisions (revised 1 October 2022)
New anti-scam SMS filtering solution and Mandatory SMS	The Infocomm Media Development Authority ("**IMDA**") has introduced new anti-scam filtering measures to safeguard SMS as a communication channel for customers. This involves key mobile operators using machine-	14 October 2022	IMDA's press release

Development	Summary	Date	Links
sender ID registration for organisation	reading technology to scan customers' SMSes for malicious links, which allows for the upstream filtration of potential scam messages. The use of such technology also allows for the detection of suspicious phrases, keywords and formats typical of fraudulent messages. For messages that require further human assessment, personal data will be stripped by the machine before it is channelled to the relevant technical personnel for review. Additionally, the IMDA will also implement a new mandatory SMS Sender ID Registration scheme to further improve Singapore's anti-scam capabilities. Organisations that intend to use SMS sender IDs in their SMS messages to Singapore mobile users will be required to register with the Singapore SMS Sender ID Registry ("**SSIR**") with effect from 31 January 2023. For a period of approximately 6 months after 31 January 2023 ("**transition period**"), all SMS messages with non-registered SMS sender IDs will be channelled to a sender ID with the header "Likely-SCAM", which is akin to a spam filter/bin. After the transition period, only SMSes with registered sender IDs will be transmitted and all other sender IDs will be blocked.		
Creation of Global Forum on Cyber Expertise Southeast Asia Liaison Position	The Cyber Security Agency of Singapore ("**CSA**") has partnered with the Global Forum on Cyber Expertise ("**GFCE**") to create a GFCE Southeast Asia Liaison position. The Liaison will connect the Southeast Asian region more closely with other GFCE member nations and organisations for greater effectiveness in international cyber capacity building efforts. The integration through the Liaison is expected to facilitate exchange of best practices, to foster a deeper understanding of the cyber capability gaps in the region and to ensure improved coordination to close such gaps.	19 October 2022	CSA's press release
Establishment of the Inter-agency Task Force to Counter Ransomware Threats	In response to the rise in ransomware cases in Singapore, the Singapore Government has convened an inter-agency Counter Ransomware Task Force ("**CRTF**"). The CRTF will recommend strategies the government can adopt to improve Singapore's national counter-ransomware capabilities (such as developing and making recommendations on possible policies, operational plans, and capabilities) and push for greater international cybersecurity cooperation.	19 October 2022	CSA's press release
Launch of Internet Hygiene Portal	The Cyber Security Agency of Singapore ("**CSA**") has launched an internet hygiene portal ("**IHP**") as a one-stop cybersecurity platform to provide enterprises with easy access to resources and self-assessment tools. The IHP also allows enterprises to perform health checks on their website or email connectivity. The IHP further aims to help consumers make informed choices to better safeguard their digital transactions from cyber threats by providing visibility on the cyber hygiene of digital platforms – an Internet Hygiene	19 October 2022	Internet Hygiene Portal CSA's press release

Development	Summary	Date	Links
	Ratings table with a simplified view of each digital platform's internet hygiene is published for the public's perusal.		
Establishment of ASEAN Regional Computer Emergency Response Team	At the ASEAN Ministerial Conference on Cybersecurity on 20 October 2022, Mrs Josephine Teo, the Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, announced further developments in the establishment of the ASEAN Regional Computer Emergency Response Team ("**CERT**") and circulated a draft Operational Framework. The ASEAN Regional CERT, which is targeted to be established in 2023/2024, aims to: – strengthen ASEAN's cybersecurity incident response coordination; and – Critical Information Infrastructure (CII) protection cooperation.	20 October 2022	CSA's press release Speech by Minister for Communications and Information
New Cybersecurity Labelling Scheme for Medical Devices	The Cyber Security Agency of Singapore ("**CSA**") has launched a new Cybersecurity Labelling Scheme for Medical Devices, which rates medical devices according to their levels of cybersecurity. This scheme aims to enable consumers and healthcare providers to make informed decisions about the use of such devices, which are increasingly connected to networks and thus potentially pose greater cybersecurity risks.	20 October 2022	CSA's press release
Singapore and Germany Sign Mutual Recognition Arrangement on Cybersecurity Labels for Consumer Smart Products	The Cyber Security Agency of Singapore ("**CSA**") has signed a Mutual Recognition Arrangement ("**MRA**") with Germany's Federal Office for Information Security. Under this MRA, smart consumer products issued with either Singapore's Cybersecurity Label or Germany's IT Security Label will be mutually recognised in both countries.	20 November 2022	CSA's press release
Singapore and Korea sign the Korea-Singapore Digital Partnership Agreement	Singapore and the Republic of Korea have signed the Korea-Singapore Digital Partnership Agreement ("**KSDPA**") to strengthen cooperation between the two countries in new emerging technological areas such as Personal Data Protection, E-payments, Artificial Intelligence and Source Code protection. The KSDPA aims to facilitate secure cross-border data flows and enable consumers and businesses to navigate the digital economy with greater ease and security.	21 November 2022	Ministry of Trade and Industry Singapore, Ministry of Communications and Information and IMDA joint press release
Release of the Counter Ransomware Task Force's report	On 30 November 2022, the CRTF published its first CRTF Report, which: – sets out the CRTF's consolidated model of the ransomware kill chain. This aims to achieve a common understanding between Government agencies of the stages of a ransomware attack;	30 November 2022	CSA's press release

Development	Summary	Date	Links
	– clarified Singapore's position on paying ransoms to ransomware attackers as being strongly discouraged; and – recommended that the Singapore Government focuses on four pillars of action to address the ransomware threat effectively. The four pillars of action are as follows: – strengthen defences of potential targets (such as Government agencies, critical information infrastructure, and businesses, especially small and medium enterprises) to make it harder for ransomware attackers to launch successful attacks; – disrupt the ransomware business model to reduce the pay-off for ransomware attacks; – support recovery so that victims of ransomware attacks do not feel pressured to pay the ransom, which fuels the ransomware industry; and – work with international partners to ensure a coordinated global approach to countering ransomware.		
Signing of Korea-Singapore Artificial Intelligence Memorandum of Understanding	To strengthen digital trade architecture and deepen digital connectivity, especially though collaborations in new and emerging technologies such as Artificial Intelligence ("**AI**"), Singapore and the Republic of Korea have signed the Korea-Singapore AI Memorandum of Understanding ("**MOU**"). The MOU is a milestone in the current digital partnership between both countries as it will allow for the exchange of AI technologies and experiences in promoting responsible AI use.	6 December 2022	Ministry of Communications and Information's press release

Slovakia

Contributors

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

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

Development	Summary	Date	Links
Cookies: Opinion of the Regulatory Authority for Electronic Communications and Postal Services of the Slovak Republic on the newly established practice	As of February 2022, new legislation on cookies is in force and effective in the Slovak Republic. The previously applicable "opt-out" principle has been replaced by the "opt-in" principle of consent. In practice, this means that the user of a terminal device must actively give unambiguous consent to the website operator to receive and store cookies (except for technical cookies). The Regulatory Authority for Electronic Communications and Postal Services of the Slovak Republic ("**the Authority**") published an opinion on the issue of obtaining consent in November 2022. The opinion was prepared in cooperation with the Office for Personal Data Protection of the Slovak Republic. In the respective opinion, the Authority describes the current practice of the website operators, highlights incorrect approaches to this matter (including examples) and describes how the new legislation should manifest itself in practice. An incorrect approach is, for example, a cookie banner/barrier covering the whole screen, which makes access impossible without essentially forcing consent to access the requested website, or if the banner - if the website operator processes and stores non-technical cookies - has an 'I understand' button (incorrect) instead of 'I accept' or 'I agree' (correct). Thus, the language or the wording of the cookie banner itself may also be an essential element. On the other hand, a recommended approach is, for example, to allow acceptance and rejection of cookies (both all and each type individually) via the cookie banner. The latter should contain the necessary information on the subject, while a link to the cookie policy, where the subject is described in more detail, is acceptable. At the same time, the Authority has pointed out that website operators often fail to recognise that, just as easily as the end-user has given	28 November 2022	Opinion of Regulatory Authority (in Slovak)

consent, they must be able to withdraw it. The ideal solution is to place the relevant button directly on the website or in the cookie policy section that the website should contain.

In the event of a breach or failure to comply with an obligation under the relevant provision of the Electronic Communications Act, the penalty may be up to 10% of the turnover of the undertaking for the preceding financial year.

South Africa

Contributors

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

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

Development	Summary	Date	Links
Information Regulator confirms Enforcement Committee fully in force, and POPIA Regulations under review	On 26 October 2022, the Information Regulator provided an update, via Twitter, of the Information Regulator's recent activities. The Regulator confirmed that the Enforcement Committee ("**Committee**"), established in August 2022, is in full force, and that numerous complaints have been referred to the Committee. The majority of complaints received are in relation to direct marketing by means of unsolicited electronic communication. The Information Regulator further indicated that: – it is establishing a security compromises and data breach unit; – an online complaints system will be established; and – the Regulations under the Protection of Privacy Information Act are under review.	26 October 2022	Information Regulator SA Twitter statement
Information Regulator approves codes of conduct from (i) the Banking Association South Africa, and (ii) the Credit Bureau Association	In terms of the provisions of section 61 (2) of the Protection of Personal Information Act, No 4 of 2013 ("**POPIA"**), the Information Regulator gave notice that it is in receipt of codes of conduct from: – Code of conduct from the Banking Association South Africa ("**BASA**") – Approved, 12 October 2022 – Code of conduct from the Credit Bureau Association ("**CBA"**) – Approved, 12 October 2022 The purpose of the codes is to: – promote appropriate practices by members of BASA and CBA, respectively, governing the processing of personal information in terms of POPIA; – encourage the establishment of appropriate agreements between members of BASA and CBA, respectively, and third parties,	Date of notification of approved Codes of Conduct in Government Gazette: 26 October 2022 Date that codes come into force - 28 days after notification: 4 November 2022	Code of Conduct for the BASA Code of Conduct for the CBA

Development	Summary	Date	Links
	regulating the processing of personal information as required by POPIA, and dictated by good business practice; and – to establish procedures for members of BASA and CBA, respectively to be guided in their interpretation of principally POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against credit bureau to be considered and remedial action, where appropriate, to be taken. The codes of conduct govern: – the processing of personal information (including consumer credit information) by credit bureau that (i) are members of BASA (in compliance with POPIA and the Banks Act, 94 of 1990), and (ii) are members of CBA (in compliance with POPIA and the National Credit Act, 34 of 2005); – where appropriate, agreements that may need to be concluded between members of BASA and CBA, respectively, and third parties promoting, and to the extent possible ensuring that personal information is processed in compliance with POPIA; and – the enforcement by BASA and CBA, respectively, of the provisions of their respective codes of conduct.		

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 grants a company permission to conduct criminal background checks and provides important clarity on employer's legitimate interest to process criminal background checks	The Swedish Authority for Privacy Protection (the "**Swedish DPA**") has granted a company permission to conduct criminal background checks on behalf of employers and other customers. In accordance with Article 10 GDPR and national data protection legislation, the Swedish DPA is authorised to grant specific data controllers the permission to process personal data relating to criminal convictions and offences. For the first time since the GDPR came into force in Sweden, the Swedish DPA has allowed a company that provides criminal background check services to process such data. These permissions have previously only been given to banks and other financial institutions that are subject to KYC obligations pursuant to anti-money laundering regulations. In the decision, the Swedish DPA also concluded that the company who conducts the criminal background checks is considered the data controller. This is the case even if the processing is ultimately performed on behalf of a customer, and despite the fact that the customer is the one who provides the initial information on the data subject that is being checked. This conclusion is reached primarily on the basis that the service provider independently determines which personal data should be included, and which processing operations are to take place, to conduct the background checks. Furthermore, it has clarified that employers can only perform criminal background checks on consultants and job candidates. Thus, employees are excluded. The Swedish DPA also states that employers are not able to rely on consent as a legal basis to conduct background checks in relation to these two groups. Lastly, the decision provides concrete examples of which types of crimes, and in relation to which categories of jobs, may fall within scope of the employer's legitimate interest to conduct a criminal background check. For example, a screening for drug and traffic offenses is allowed for	3 October 2022	Press statement (in Swedish) Decision (in Swedish)

Development	Summary	Date	Links
	positions in which the individual must drive a vehicle (for example, truck drivers).		
Swedish DPA grants a bank the permission to process personal data relating to criminal convictions and offences and provides important clarity on when data controllers subject to Swedish anti-money laundering regulations can process such data	The Swedish DPA has allowed a bank operating in Sweden to process personal data relating to criminal convictions and offences. The permission also covers the bank's intention to share their background checks on existing and potential customers with other bank branches belonging to the same company group. Of greater importance, is that the Swedish DPA concluded that data controllers, who must assess customer risk profiles pursuant to the Swedish Anti-Money Laundering Act (2017:630), are not allowed on this basis alone to process personal data relating to criminal convictions and offences. In other words, Swedish banks and other financial institutions must receive permission from the Swedish DPA prior to processing such data. The requirement to receive a permission from the Swedish DPA would therefore also include screening customers against sanctions lists, at least to the extent such processing is necessary to assess a customer risk profile. The decision highlights the opposing interests between anti-money laundering obligations and data privacy. It was closely followed by the EU court's ("**CJEU**") decision in the joined cases C-37/20 and C-601/20 to restrict the public's access to information on companies' real owners under the EU directive on anti-money laundering.	6 October 2022	Press statement (in Swedish) Decision (in Swedish)
Swedish DPA initiates audit on a company due to data breach of a digital school platform	After receiving approximately 60 notifications of personal data breaches from schools and municipalities, the Swedish DPA initiated an audit on a company that provides a digital school platform for students, parents and teachers. According to the notifications, an unknown threat actor had gained unauthorised access to personal data relating to students and teachers and downloaded the information from the digital school platform. The Swedish DPA has asked the company responsible a number of questions to find out what happened, including how the company discovered the incident, the extent of the breach, as well as what organisational and technical security measures were put in place before and after the incident.	19 October 2022	Press statement (in Swedish) Audit statement (in Swedish)
The Swedish Government delivers in its proposal an increased budget for the Swedish DPA	The Swedish Government has, in its budget proposal, increased the Swedish DPA's overall budget by SEK 56 million over the next two years. As a result of this increased funding, the Swedish DPA has decided to recruit approximately 50 more employees. These recruitments will mainly	24 November 2022	Press statement 1 (in Swedish) Press statement 2 (in Swedish)

Development	Summary	Date	Links
	consist of additional lawyers, but also IT and information security specialists and administrative personnel. Once the recruitments are completed, the Swedish DPA will have a total of approximately 150 employees and as of 2024, and an annual budget of approximately SEK 180 million.		
Swedish DPA publishes a report on Swedes' knowledge of GDPR	The Swedish DPA has published a report titled "Digital Privacy 2022" based on a survey that consisted of 1,000 web interviews with individuals between the ages of 18 to 79. The report reveals, among other things, that only half of Swedes know about GDPR and only one in five protects their personal data. According to the report, most Swedes are comfortable with the way public authorities use their personal data, while a third of the surveyed individuals worry about the processing done by companies. Furthermore, the report states that six out of ten rarely, or never, read a company's terms of service.	29 November 2022	Press statement (in Swedish) Report (in Swedish)
Swedish DPA publishes guidance on data privacy analysis	The Swedish DPA has published guidance on data privacy analysis. The guidance is primarily aimed at stakeholders who prepare draft legislation or governance proposals that involve processing of personal data, but may also be useful for other purposes such as implementing a high risk processing activity. The guidance is structured in seven steps and includes examples of questions that may need to be answered and documented, as well as suggested measures that can be taken to reduce privacy risks. A checklist is also included which describes the following steps of a data privacy analysis: – identify the relevant data processing and assess which regulatory frameworks are applicable; – identify and assess the privacy risks that can arise from the relevant data processing; – identify existing legislation that can provide a legal basis for the relevant data processing; – identify and assess the need for new legislation; – assess whether the Swedish constitution regarding certain right to privacy from public authorities comes into conflict with the proposed legislation;	7 December 2022	Press statement (in Swedish) Report (in Swedish)

Development	Summary	Date	Links
	– assess how the proposed legislation should be designed, taking into account applicable data protection legislation; and – conduct a final assessment on the principles of proportionality and necessity.		
Administrative fine issued by the Swedish DPA against search engine operator becomes legally binding	Back in March 2020, the Swedish DPA issued an administrative fine of SEK 50 million against a search engine operator due to the company's routine of informing webmasters when a search match had been removed from the list of search results. This procedure was, according to the Swedish DPA, in breach of the right to be forgotten as stipulated under the GDPR. The decision has subsequently been appealed to the Gothenburg administrative court and the administrative court of appeal. In both cases the administrative fine was upheld. The Supreme Administrative Court has now denied further appeal, which means that the court decision by the lower instance has become legally binding.	21 December 2022	Press statement (in Swedish)

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
New data protection legislation creating obligation to appoint a representative in Switzerland comes into force in September 2023	As a result of the new data protection legislation coming into force in September 2023, there will be an obligation to appoint a representative in Switzerland. Private controllers (companies or private persons that decide on the purpose and the means of the processing of personal data) with their domicile or residence outside of Switzerland have to designate a representative in Switzerland if they process personal data of persons in Switzerland and the data processing fulfils the following requirements: – the data processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of these persons; – the processing is extensive; – it is a regular processing; and – the processing involves a high risk to personal data of the data subjects. The appointed representative will serve as a contact point for the data subjects and the Federal Data Protection and Information Commissioner ("**FDPIC**"). The controller will have to publish the name and address of the representative. The representative will have the following duties: – the representative's office shall keep a register of the processing activities of the controller;	21 December 2022	Statement (in German)

Development	Summary	Date	Links
	– on request, it shall provide the FDPIC with the information contained in the register; and – on request, it shall provide the data subject with information on how to exercise his rights.		
Information Security Act ("ISA") expected to come into force in mid-2023	The ISA was adopted in December 2020 in the final vote after three years of consultation. The ISA and the implementing regulations are expected to come into force in mid-2023. The purpose of the ISA is to ensure the secure processing of information for which the Confederation is responsible and the secure use of the Confederation's IT resources. It is intended to replace and consolidate the current fragmented legal basis set out in a multitude of decrees. The ISA will primarily be applicable to the Confederation, especially the Federal Administration (including the Federal Courts and the Federal Assembly). It will also apply to cantonal authorities if they process classified information of the Confederation or access its IT resources. To ensure information security, the ISA provides for "general measures" at several levels: – The obligated organisations are first generally obliged to ensure information security, i.e. in particular for the confidentiality, verifiability and integrity of the information in their area of responsibility and for the traceability of its processing. – Furthermore, information must be classified and, according to its classification, only made accessible to authorised authorities. – In the use of IT resources. For this purpose, the ISA defines security levels (basic protection, high protection and very high protection) and requires the obligated authorities to provide for corresponding graduated minimum requirements. – In the deployment of personnel, the selection, identification, education and training and obligation to maintain secrecy must be regulated accordingly, and a "need-to-know principle" must generally be observed. – Physical protection must be ensured to protect information and IT resources. – Identity management systems (i.e. central administration of personal identification) are regulated. Detailed regulations then apply to personal security audits, to the operational security procedure (i.e. an audit of third parties who come into consideration for the fulfilment of public contracts and would thereby	21 December 2022	Statement in German

Development	Summary	Date	Links
	perform a security-sensitive activity, so-called "security-sensitive contracts", as such an audit is currently only established for military procurements) and for critical infrastructures.		

United Kingdom

Contributors

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

Jonathan Palmer
Senior Associate
T: +44 20 7919 4879
jonathanpalmer@
eversheds-sutherland.com

Development	Summary	Date	Links
Plan to replace UK GDPR	On 3 October 2022, the Secretary of State for Digital, Culture, Media & Sport ("**DCMS**"), Michelle Donelan, outlined plans to replace the UK GDPR with a new data protection system, to remove the "unnecessary red tape" of the EU inherited GDPR. Ms Donelan explained that the government would look to countries who achieve data adequacy without having GDPR, like Israel, Japan, South Korea, Canada and New Zealand, when designing the British new system. The key aims of the reforms include to "protect consumer privacy and keep their data safe, whilst retaining our data adequacy so businesses can trade freely".	3 October 2022	'Our plan for digital infrastructure, culture, media and sport'
The final Online Advertising Programme market insights report has been published by DCMS	The Department of Digital, Culture, Media & Sport ("**DCMS**") has released the final version of the 'Online Advertising Programme Market Insights' report. The report considered a number of topics including, but not limited to, online advertising harms, market trends, supply chains and international regulatory developments (both within the EU and the US). The report set out a number of categories of ways in which online advertising can harm consumers and the industry, such as being misleading, offensive, fraudulent, malicious, targeting vulnerable people or being discriminatory in their targeting. According to the report, 35,115 Action Fraud reports were raised concerning online fraudulent advertisements in 2020/21. Due to the changing nature of online advertising and the rise of social media platforms, the report shows that complaints concerning social influencer advertising have increased considerably, with Advertising Standards Authority complaints growing by 92% in 2021. Interestingly, the findings showed that consumer harm has decreased in certain areas where protection measures have strengthened in recent years, for example paid search advertising for investment scams appear	30 September 2022	Online Advertising, Programme Marketing Insights – Final Report

Development	Summary	Date	Links
	to have decreased following the introduction of verification measures in August 2021. The market trends section of the report showed the extent of growth of online advertising expenditure and the new methods of advertising that have been emerging through social media, connected TV advertising, digital audio and in-game advertising (to name a few).		
The ICO has launched a consultation on the draft employment practices: monitoring at work guidance and draft impact assessment	The ICO has issued draft guidance on 'employment practices: monitoring at work', along with an impact scoping document setting out the potential impacts of the draft guidance that it has considered so far. The ICO explains that monitoring practices have changed substantially since it published its employment practices code in 2011, especially during the pandemic. The draft guidance says: "The UK GDPR and the DPA 2018 do not prevent monitoring. They set out a framework for the collection and use of personal data. You must balance the level of intrusion against the needs of the employer, workers and members of the public". The draft guidance covers a number of topics, including how to lawfully monitor workers. Consultation is open until 11 January 2023.	12 October 2022	ICO consultation
The ICO has launched a consultation on Children's Code evaluation	On 30 September 2022 the ICO launched a consultation requesting the opinions of stakeholders and the public on the Children's Code. The Children's Code is a code of practice guiding best practice for online services that are likely to attract use by children. The Code originally came into force on 2 September 2020, with the ICO requiring compliance by organisations by 2 September 2021. The ICO is now reviewing the Code's effectiveness to determine its impact. As part of the consultation, the ICO is requesting information from various sources, including conducting market research and engaging with stakeholders, as well as considering the ICO's own experience of the Code and its supervision of compliance throughout the past year. Consultation responses must be submitted by 5pm on Friday 11 November 2022. The ICO will feed views into a report that will subsequently be released on this topic.	30 September 2022	ICO consultation
ICO publishes updated guidance on transfer risk assessments	The Information Commissioner's Office (**"ICO"**) published the International Data Transfer Agreement ("**IDTA**") earlier this year, alongside the Addendum to the EU's Standard Contractual Clauses (**"Addendum"**). The ICO has now **published** updated guidance on	17 November 2022	ICO guidance: International Transfers

Development	Summary	Date	Links
	international data transfers to include a section on transfer risk assessments ("**TRAs**") and a new TRA tool. These constitute the UK's approach to TRAs (on which the European Data Protection Board ("**EDPB**") has previously provided guidance to EU Member States). The aim is to "find an alternative, achievable approach delivering the right protection for the people the data is about, whilst ensuring that the assessment is reasonable and proportionate". The ICO has published a 6 question TRA tool that provides a method to assess the risk level for different categories of personal data. The ICO has notably shifted TRAs to focus in particular on whether the transfer significantly increases the risk of a privacy/human rights breach. The ICO has said it is also developing clause by clause guidance on using the IDTA and the Addendum, and is considering making further updates to the TRA guidance to include worked examples.		
ICO issues warning on use of emotional analysis technologies	The ICO has issued a warning to organisations that use, or are considering use of, emotional analysis technologies. It is recommended that a thorough risk assessment is undertaken to assess the public risks before any systems are implemented. Emotional analysis technologies are technologies that process and analyse certain data such as eye and facial movements, sentiment analysis, gait analysis, heartbeats, expressions and skin moisture. This kind of technology may be used where employers are monitoring the health of their employees through 'wearable screening tools', or for monitoring the body language and expressions of students being registered for exams. The ICO predicts that biometrics will have a major impact on a number of key sectors, including finance and commercial, fitness and health and employment. Artificial intelligence and biometrics technology has grown considerably, and these developments have been described by the Deputy Commissioner Stephen Bonner as being 'immature' and despite bringing some opportunities, they bring 'greater risks' to people's privacy rights. The ICO has stated that it has not yet seen any technologies of this kind that meet data protection requirements and comply with the proportionality, fairness and transparency requirements set out within the law. The ICO wishes to assist organisations which wish to utilise these technologies to advance their business innovation and growth, whilst taking action where required. The ICO is currently drafting a biometric guidance document that is due to be published in Spring 2023. This will	26 October 2022	ICO warning

Development	Summary	Date	Links
	provide organisations with clarity on the data protection principles that must be complied with when using these technologies.		
ICO consultation on prioritisation of FOIA complaints	The ICO has launched a consultation on how it prioritises complaints about requests made to public bodies under the Freedom of Information Act ("**FOIA**"). The consultation closes on 19 December 2022. Its proposal is to prioritise complaints where there is an explicit public interest in the information that has been asked for. Public interest includes different values and principles relating to the public good. Suggested criteria include: – "Is there a high public interest in the information requested? Does it raise a novel or clearly high-profile issue that we should look at quickly? – Is the requester a person or group who is raising information rights awareness, supporting vulnerable groups or raising awareness of potentially significant public interest issues? – Are vulnerable groups or people potentially significantly affected by the information requested? – Would prioritisation have significant operational benefits or support those regulated?" The proposed prioritisation criteria would cover complaints made under both the FOIA and the Environmental Information Regulations. The ICO states that this new system would enable it to aim to allocate priority cases within 4 weeks and to complete 90% of all cases within 6 months which would be much swifter than the current timescales.	8 November 2022	ICO consultation
ICO guidance and FAQs on how to use AI appropriately and lawfully	The Information Commissioner's Office (ICO) has recently published guidance and frequently asked questions on using AI and personal data appropriately and lawfully. The use of AI is becoming more and more prevalent among businesses but there are important data protection concerns to consider. In its guidance, the ICO makes a number of recommendations to ensure compliance with data protection laws. These include: – Take a risk based approach when developing and destroying AI; – Think carefully about how you can explain the decisions made by your AI system to individuals affected;	8 November 2022	ICO guidance

Development	Summary	Date	Links
	– Collect only the data you need to develop your AI system and no more; and – Address risk of bias and discrimination at an early stage.		
ICO publishes new direct marketing guidance and web resources	The ICO has published a new toolkit on direct marketing. It is meant to support organisations on their direct marketing activities. It is made up of various checklists and resources for organisations with marketing activities. There is, for example, general guidance as well as a simple checklist aimed at smaller organisations. There is also guidance for the public sector or data brokers, as well as a guide to the Privacy and Electronic Communications Regulations 2003 ("**PECR**"). It can be found on the ICO's website.	5 December 2022	ICO toolkit
New data protection policy note for all central government departments	On 30 November 2022, the Crown Commercial Service published the 'Procurement Policy Note 03/22: Updated Guidance on Data Protection Legislation' ("**PPN 03/22**"). The PPN 03/22 applies to 'all central government departments, their executive agencies and non-departmental public bodies'. Other public bodies may also wish to use the approaches set out in PPN 03/22 as they are subject to the same legislation. This PPN replaces the PPN 02/18, and it incorporates key developments that have been made within the data protection framework, including UK GDPR, ECJ decisions regarding personal data transfers and the approval of the Internal Data Transfer Agreement. For example, at Annex A Part 1 of the PPN 03/22 it includes 'Generic Standard UK GDPR clauses' that should be included in contracts where relevant.	2 December 2022	PPN 03/22
New Telecommunications Security code of practice	On 1 December 2022, a new Telecommunications Security Code of Practice was published and came into force. This new code of practice follows the Government's UK Telecoms Supply Chain Review Report that was published in July 2019. This report emphasised the security risks associated with developments in telecommunications networks, such as 5G and full fibre. The review determined that a new security framework was needed. Alongside this code of practice, in October this year, the Electronic Communications (Security Measures) Regulations 2022 (the "**Regulations**") also came into force. The code of practice is intended to work alongside the Regulations.	5 December 2022	Telecommunications Security Code of Practice

Development	Summary	Date	Links
	The code applies to public telecom providers, and it has come into force pursuant to the Communications Act 2003, as amended by the Telecommunications (Security Act) 2021. The code of practice is formed of three sections, setting out the following information: – Section 1 provides the context and background of the code, including legal status and how it applies to public telecoms providers. – Section 2 outlines the key concepts that must be understood by all providers when applying the security measures contained within the Regulations and the technical guidance outlined in Section 3 of the code. – Section 3 contains the technical guidance measures, mapping each measure to the relevant security measure within the Regulations. This section also explains the implementation timelines for the guidance measures.		
UK and Ukraine reach ground breaking digital trade deal	The UK and Ukraine have agreed a Digital Trade Agreement which will provide support for the Ukrainian economy. The agreement is being put in place to provide the Ukraine with the foundations to recover and revive through and from the current crisis. Digital trading is increasingly important, especially during the current conflict, and allows Ukraine to continue to trade and access vital goods and services, collaborating with businesses and governments. The deal 'facilitates cross-border data flows', and also enhances 'co-operation between the UK and Ukraine on cybersecurity and emerging technologies'. This agreement follows the UK's decision earlier in May 2022 to remove all tariffs under the UK-Ukraine free trade agreement.	7 December 2022	Government Press Release
What cyber security risks do you face when working from home?	With remote working becoming more prevalent within working patterns post pandemic, it is important to consider the cyber security risks that may be encountered when home-working. Within a recent news article 'Manchester Digital' set out the key frequently asked questions about working remotely, and included a commentary titled 'what cyber security risks do you face when working from home'. The key risks identified in the article are set out below. – Unauthorised device access - it is important to ensure devices are locked when left unattended at home as it is a cyber risk for family members to see what is on your computer screen.	5 December 2022	Manchester Digital Article

Development	Summary	Date	Links
	– Sensitive data exposure - family members and individuals that may be around you when working from home should not be able to see sensitive data, as that would constitute a breach of UK GDPR. Best practice is to have a secure storage cabinet where your work items including computers, devices, documents, paper notes and notebooks can be kept to ensure security. – Use the correct device - if a 'bring your own device' culture is promoted within your workplace, it is important to separate any work data from personal data on the device. It is recommended to use separate accounts for work and personal use and have strong and unique passwords, alongside a form of multi-factor authentication.		
"Whaling" cyber-attacks	Although phishing is still the most common type of security breach, the second most common is now known as "whaling". Whaling is when hackers aim to convince their target that they are a senior executive at their company who requires urgent assistance via payments or company information. Employees are tricked into this as the communication is typically similar to that of the company by using company graphics. A way for employees to catch whaling attempts is to check the email address or phone number from which the message is from. Typically, hackers will have changed the email address slightly or be attempting to contact an employee from an unknown number. A typical excuse used by hackers is that they are not able to speak directly on the phone, therefore the employee cannot verify the identity of the senior executive. One way to prevent whaling is to have two-factor authentication and Domain-based Message Authentication, Reporting and Conformance ("DMARC").	13 December 2022	
Increased transparency: important changes to information made publicly available by the UK's ICO	All organisations that process personal data should be aware of recent changes to the way the UK's Information Commissioner's Office ("**ICO**") publishes information: – First, the ICO has started publicly publishing details of its reprimands (that is, formal decisions made by the ICO that an organisation has infringed data privacy law, along with recommended further actions), backdated to January 2022. Previously, the ICO only published details of its more stringent actions, e.g. fines it had levied and enforcement notices ("ENs") which compelled entities to take specific actions. These reprimands, although relatively limited in number to date (under 30), contain significant detail and are likely to be of interest to both claimant law firms and journalists in the same way that fines and ENs are. Reprimands can be issued by the ICO following any sufficiently serious GDPR infringement, for example, a	December 2022	ICO published Reprimands ICO published data protection complaints ICO published actual or potential data breaches ICO published civil investigations ICO published cyber investigations John Edwards Speech

Development	Summary	Date	Links
	cyber security incident involving personal data or other GDPR personal data breach. – Second, the ICO has started publicly publishing details of 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 there is not much detail in these spreadsheets, for each entry they set out the name of the relevant controller and which Article of the GDPR was infringed or allegedly infringed (so that, for example, complaints about data subject access requests under Article 15 GDPR are easy to spot), and are therefore also likely to be of interest to claimant law firms and journalists who it's fair to assume will be scanning them regularly. While these developments are in line with the UK ICO's push toward transparency, and the publishing of reprimands at least was forewarned in a speech by John Edwards – the UK's Information Commissioner – in November 2022, they were introduced quietly at the end of 2022. Going forwards, these changes will need to be taken into account by controllers when considering whether to self-report potential data breaches (i.e. before there's a reasonable degree of certainty that there has been a data breach): self-reporting a borderline data breach "just in case" may no longer be an attractive option if that report will subsequently be made public. We would emphasise, however, that clear (i.e. "non-borderline") data breaches should continue to be reported.		
20% of operational incidents reported to FCA relate to third party failures	With the deadline for comments on 'Discussion Paper 22/3: Operational resilience: critical third parties to the UK financial sector' due 23 December 2022, we submitted a request to the FCA under the Freedom of Information Act 2000, to gain some insight into the risks arising from financial services' growing reliance on these critical third parties. Our request revealed some interesting statistics about the operational incidents that have occurred in 2022. For example, so far, 335 unique incidents have been reported under SUP 15.3 and/or Principle 11. Of these, 113 incidents related to third party failures. To learn more about our findings, read our flash briefing linked within the Links column.	December 2022	LinkedIn Flash Update

United States

Contributors

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

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

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

Rebekah Whittington*
Associate
T: +1.404.853.8283
rebekahwhittington@
eversheds-sutherland.com
(*Not admitted to practice. Application submitted to the Georgia Bar)

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

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

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

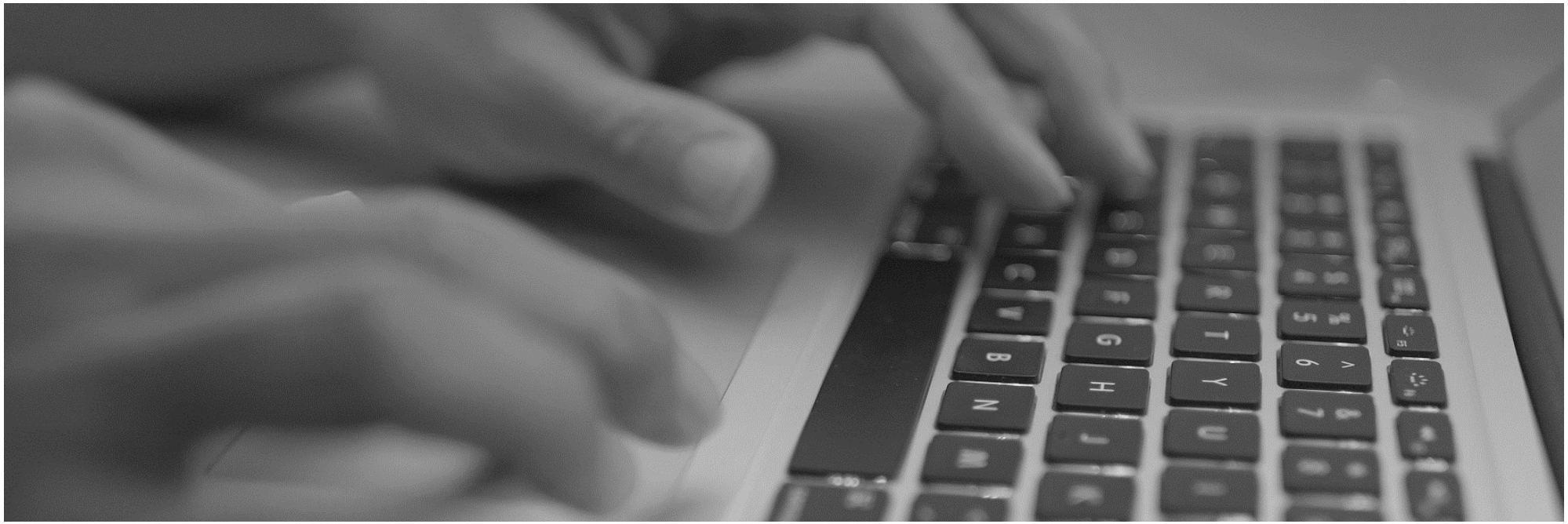
Rachel May
Associate
T: +1.202.383.0306
rachelmay@
eversheds-sutherland.com

Development	Summary	Date	Links
Software Company's Damages From Ransomware Attack Not Covered Under Business owner's Insurance Policies	On December 27, 2022, the Supreme Court of Ohio held that software company EMOI Services, LLC (EMOI) was not entitled to coverage under its insurance policy for losses arising from a ransomware attack. EMOI attempted to apply the insurance policy under the notion that the company's software is electronic equipment. However, the policy stated that there must be "direct physical loss of, or direct physical damage to, electronic equipment or media before the endorsement is applicable." "[Since] software is an intangible item that cannot experience direct physical loss or direct physical damage," the court reasoned that the attack did not meet the requirements of policy for the endorsement.	27 December 2022	Supreme Court of Ohio Decision

Development	Summary	Date	Links
Illinois Court Issues Ruling on Biometric Information Privacy Act Case Involving Retention Policy Time Limit	On November 30, 2022, an Illinois court issued a ruling in *Mora v. J&M Plating, Inc.*, involving the retention policy time limit under the state's Biometric Information Privacy Act ("**BIPA**"). In its ruling, the court held that BIPA requires private entities to develop a retention-and-destruction schedule upon possession of biometric data. This ruling emphasizes the importance of establishing retention policies *prior* to collecting data.	30 November 2022	Illinois Court Ruling
Pennsylvania Amends Its Breach of Personal Notification Act	On November 3, 2022, Pennsylvania's Governor signed Senate Bill 696, amending the state's data breach notification law to expand the definition of personal information and provide a new method for data breach notification. Taking effect May 2, 2023, the amendments include: – An expansion of the definition of personal information to include: (1) medical information (any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional), (2) health insurance information (an individual's health insurance policy number or subscriber number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits), and (3) a username or email address, in combination with a password or security question and answer that would permit access to an online account; – A Health Insurance Portability and Accountability Act ("**HIPAA**") exception to compliance with the law; and – A new permissible method of providing notice of a breach: if the affected personal information consists of a username or email address in combination with a password, electronic notice will now be permitted, as long as the notice directs the affected individual to promptly change their security question and password, or take other steps to protect their online account.	3 November 2022	Pennsylvania Senate Bill 696
SEC Proposes Service Provider Oversight Requirements for Investment Advisers	On October 26, 2022, the Securities and Exchange Commission ("**SEC**") proposed new Rule 206(4)-11 under the Investment Advisers Act of 1940 ("**Advisers Act**"), which would prohibit SEC-registered investment advisers from outsourcing certain services or functions to service providers without meeting minimum requirements. At the same time, the SEC also proposed certain related amendments to Rule 204-2 under the Advisers Act and Form ADV. Proposed Rule 206(4)-11 ("**Proposed Rule**") would require investment advisers to conduct due diligence prior to engaging a service provider to perform certain services or functions. It would further require advisers to	26 October 2022	Proposed Rule 206(4)-11

Development	Summary	Date	Links
	periodically monitor the performance and reassess the retention of the service provider in accordance with due diligence requirements to reasonably determine that it is appropriate to continue to outsource those services or functions to that service provider. The proposed amendments to Form ADV are intended to collect census-type information about the service providers defined in the proposed rule. In addition, the proposed amendments to Rule 204-2 would include a new provision requiring any adviser that relies on a third party to make and/or keep books and records to conduct due diligence and monitoring of that third party and obtain certain reasonable assurances that the third party will meet certain standards.		
New York Department of Financial Services settles with EyeMed Vision Care LLC	On October 18, 2022, the New York Department of Financial Services ("**NY DFS"**) announced that it had settled with EyeMed Vision Care LLC ("**EyeMed**") for the company's violation of the NY DFS data protection regulations. On October 9, 2020, EyeMed reported a one-week breach to the NY DFS. During the breach, an intruder was able to access emails and attachments dating back six years before the attack. As a result, the attackers were able to access the information of over 2 million customers, including children. EyeMed suggested that the breach was likely the result of a successful phishing scheme. NY DFS investigated EyeMed to determine whether the company had violated Cybersecurity Regulation 23 NYCRR Part 500. In its investigation, the NY DFS determined that EyeMed failed to implement multifactor authentication, limit user access privileges, implement sufficient data retention and disposal processes, and conduct a risk assessment that complied with the regulation. EyeMed agreed to pay the NY DFS a $4.5 million penalty and undertake significant remedial measures to better security its data.	18 October 2022	NY DFS Consent Order to EyeMed
President Biden Signs Executive Order on Enhancing Safeguards for the United States Signals Intelligence Activities	On October 7, 2022, President Biden signed an executive order on "Enhancing Safeguards for the United States Signals Intelligence Activities," which establishes new regulations for the collection and use of personal data by U.S. intelligence agencies. The executive order is intended to provide greater privacy protection to help re-establish an EU-U.S. framework for the legal export of personal data from the EU to the U.S. under EU laws, following the 2020 *Schrems II* decision that invalidated the prior privacy framework (**"Privacy Shield"**) between the two jurisdictions. Among other reforms, the executive order implements a new two-tier redress mechanism for privacy violations where individuals can lodge	7 October 2022	Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities Regulations Establishing the Data Protection Review Court

Development	Summary	Date	Links
	complaints with the civil liberties protection officer ("**CLPO"**), who is appointed by the director of national intelligence. The CLPO will then launch an investigation to determine whether the order's safeguards or other US laws have been violated and the proper remediation. If the complainant is dissatisfied with the outcome, they can appeal the decision to a Data Protection Review Court ("**DPRC"**) under the second tier of the redress mechanism. The regulations establishing the new court require a three-panel judge to review applications. In addition, the DPRC must appoint a special advocate to represent the complainant at the court. The Privacy and Civil Liberties Oversight Board ("**PCLOB"**) will be *encouraged* to review this two-tier redress mechanism on an annual basis.		



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:

Jonathan Palmer
Senior Associate
T: +44 20 7919 4879
jonathanpalmer@eversheds-sutherland.com

Rebecca Crowe
Trainee Solicitor
T: +44 1223 44 3890
rebeccacrowe2@eversheds-sutherland.com

Alina Brenninkmeijer
Trainee Solicitor
T: +44 2079 19 0971
AlinaBrenninkmeijer@eversheds-sutherland.com

Asmee Dutt-Choudhury
Trainee Solicitor
T: +44 121 232 1022
AsmeeDutt-Choudhury@eversheds-sutherland.com

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

eversheds-sutherland.com

Updata Edition 18