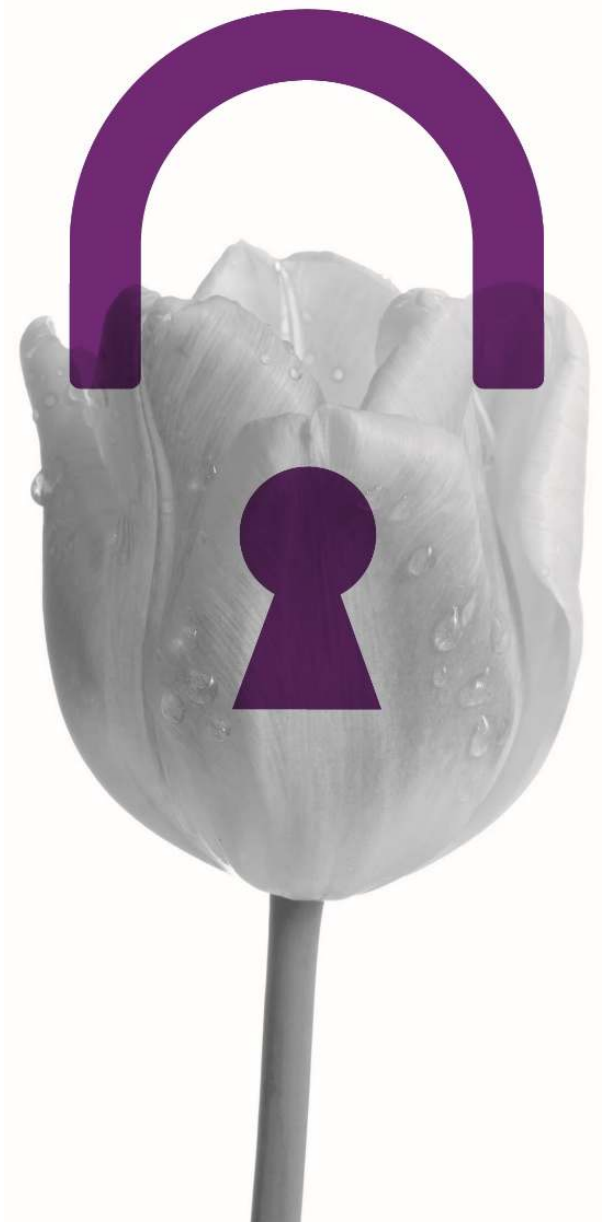
EVERSHEDS SUTHERLAND



Updata

Your quarterly Data Privacy and Cybersecurity update

April to June 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.

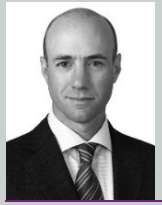
This edition covers April to June 2022 and is full of newsworthy items from our team members around the globe, including:

- Connecticut becomes the fifth US state to pass an enhanced data privacy law, while the US Federal Trade Commision, with the Senate confirmation of Commisioner Bedoya in May, is poised for greater privacy enforcement action and rulemaking;
- the development of caselaw and guidance on health data (particularly covid 19 status and vaccination status) examples include cases from the Netherlands and Belgium, new guidance from the Irish and Spanish regulators, directions to delete Covid 19 data from a German regulator and the development of security requirements for managing health data in public health crises in China;
- continued scrutiny of cross border transfers to the US (particularly out of Austria) and the development of cross-border transfer model clauses from the Hong Kong regulator;
- some useful clarification on calculating the impact on data subjects from personal data breaches involving personal identification numbers from the Polish regulator;
- the lawful use of cookies continues to attract regulatory attention with important developments in Austria, Belgium and Germany;
- cybersecurity continues to be a focus for regulators, with the launch of certification standards (Singapore) and audits by regulators (Austria and Germany);
- both the Irish and UK regulators have provided updated guidance on the use of children's data;
- the use of drones has incurred fresh regulatory scrutiny from regulators in Hungary and Ireland; and
- our Chinese colleagues have set out the development on the continued expansion and further public consultation of regulation on cybersecurity, AI and Big Data in China.

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

Sarah Thorley
Associate
T: +44 1223 44 3782
sarahthorley@
eversheds-sutherland.com

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

Development	Summary	Date	Links
Max Schrems pens open letter to the EU Commissioner for Justice and others, providing preliminary observations and potential legal challenge in response to the Trans-Atlantic Data Privacy Framework	Following the March 2022 announcement of an agreement in principle addressing the new Trans-Atlantic Data Privacy Framework, an open letter of observations and potential legal challenge from Max Schrems (the lead plaintiff in the *"Schrems I"* and *"Schrems II"* cases), has recently been sent to the EU Commissioner for Justice, the U.S. Secretary of Commerce, Pauline Dubarry, the European Data Protection Board Chair, and Chairman of the Committee on Civil Liberties, Justice and Home Affairs. The letter was published to the public by '*None of Your Business*' ("NOYB") – the European Centre for Digital Rights, a non-profit organisation based in Vienna to which Schrems is the Honorary Chairman. Within the letter, Schrems particularly discusses suggestions relating to the lack of reforms on US surveillance and laws, as well as providing a caution that there is a need for general commercial data protection obligations to be improved. The body of the letter addresses three main areas: **1.** Applying a correct proportionality test on US surveillance law under Article 8 CFR; **2.** Creating meaningful judicial redress under Article 47 CFR;	23 May 2022	Press Release Letter

Development	Summary	Date	Links
	and **3.** The need to update commercial privacy protections. The letter also goes on to criticise the proposed framework's ability to protect human rights to privacy and data protection in future trans-Atlantic data transfers. Although it is stated that the purpose of the letter was to provide a useful overview of observations which may significantly impact the proposed plans for the Trans-Atlantic Data Privacy Framework, Schrems does refer to potential litigation should any final decisions "*fail to provide the needed legal certainty*".		
European Commission publishes a Q&A on Standard Contractual Clauses	The European Commission has published a Q&A on the two sets of Standard Contractual Clauses ("SCCs") on controllers and processors and third-country data transfers adopted on 4 June 2021. The Q&A is intended to provide practical guidance on the use of SCCs to ensure compliance and has been formulated following stakeholder feedback. An outline of the rationale behind the adoption, methods to evaluate their success and the practical implications of the SCCs are covered in the Q&A for both SCCs. The questions cover a wide range of topics including the obligations of data exporters and importers, the scope of application for different transfer scenarios, redress for violation of the SCCs and the application of local laws including the *Schrems II* judgment. Whilst the FAQs cover familiar ground and the level of helpfulness in resolving the questions is debatable, these FAQs are worth reading. Several points are "known already". For example they confirm that new transfers SCCs are being progressed to cover the gap where the importer is subject to the GDPR, though there is no time line yet. More helpfully they comment on interpretation of the SCC and some flexibility on how to document onward transfers. Perhaps unhelpfully, they also comment on limitation of liability, and here cause more debate than resolution by commenting at Q35 that other clauses in the broader (commercial) contract (e.g. special rules on the distribution of liability, liability caps in the relationship between the parties) may not contradict or undermine the liability schemes of the SCCs. We're already seeing this add fuel to already heated debate on whether that means no limitation at all (even between the contracting parties) or just not so much as to	25 May 2022 (Happy 4 year birthday GDPR!!)	Q&A

Development	Summary	Date	Links
	undermine the operation of the clause and make them meaningless.		
MedTech publishes its response to EU Cyber Resilience Act impact assessment.	MedTech Europe ("MedTech") has published its response to a call for evidence from the European Commission in respect of its proposal for a Regulation on horizontal cybersecurity requirements for digital products and ancillary services (Cyber Resilience Act). The response outlines the current role of legislation in this regard, specifically the Medical Devices Regulation and the In Vitro Diagnostic Medical Devices Regulation. MedTech notes that the existing legislation provides for requirements on medical technologies that ensures they afford innovative safety and security to users and patients. It is further notes that any further regulatory measures consider these existing legislative requirements as sectors such as software design are already well accounted for and fragmentation may result from any regulatory misalignment. In addition to the existing legislative landscape MedTech recommends the development of organisation wide and specific cybersecurity strategies, ringfencing funding for training and wider investments in cybersecurity and training both at organisational levels and within formal education. Lastly, MedTech urges the European Commission to consider existing work undertaken by other organisations within the field, namely the International Medical Device Regulators or and the Medical Devices Coordination Group, to promote a cohesive structure to reinforce the overall resilience of cybersecurity measures for digital products.	1 June 2022	MedTech response
The European Data Protection Board responds to joint payment industry's concerns in respect of the Guidelines 06/2020 on the interplay of the Second Payment Services Directive ("PSD2") and the General Data Protection Regulation ("GDPR").	The European Data Protection Board ("EDPB") has responded to a letter from various members of the joint payments industry which highlighted concerns in respect of the Guidelines 06/2020 on the interplay of the Second Payment Services Directive ("PSD2") and the General Data Protection Regulation ("GDPR") adopted on 17 July 2020 The EDPB notes that it does not consider revisions to the Guidelines requested by the joint payments industry necessary, as such revisions has already been considered through public	1 June 2022	EDPB response

Development	Summary	Date	Links
	consultation and stakeholder events before publication of the final version of the Guidelines. It is further noted that supervisory authorities have the competence to promote the awareness of controllers and processors of their obligations under the GDPR and that payment providers can seek advice from their national supervisory authorities if clarity and information is required on the Guidelines. The EDPB also suggests that the payment sector should prepare a code of conduct for approval by their national supervisory authority to assist with the proper application of the GDPR and services which fall under the PSD2 for specific stakeholders and their sectors.		

Austria

Contributors

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

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

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

Development	Summary	Date	Links
Austrian DPA: Second decision against use of US-based web-analytics tool: No "risk-based approach" for third country transfers under GDPR	In January 2022, the Austrian DPA ruled that an Austrian website's use of a web analytics tool of a major US-based service provider violates GDPR (see Updata Edition 15). In April 2022, the Austrian DPA issued a further decision against a different website provider, reiterating that the use of this US-based analytics tool violates GDPR, as the tools transferred personal data to the USA in violation of Chapter V of the GDPR. Furthermore, it ruled that when assessing data transfers to a third country outside of the EEA, the GDPR does not allow for a "risk-based approach" for assessing the level of data protection in the third country. The mere possibility of access to the personal data by US authorities renders the level of data protection within the USA inadequate, regardless of the probability of the US authorities actually accessing the data. So as long as access by US authorities to personal data processed by the data importer is possible under FISA 702, a data transfer to the data importer violates GDPR. Furthermore, the DPA ruled that the same applies, even if the website provider configures the analytics tool to shorten the user's IP address before transferring it to the USA.	22 April 2022	English translation of the decision (created by noyb) Link Redacted copy of the decision (in German) Link Article Link

Development	Summary	Date	Links
	The decision is not yet legally binding, as the defendant has appealed the decision.		
Austrian DPA publishes FAQs on the use of cookies and cookie banners	The Austrian DPA has published FAQs on the legal requirements for the use of cookies and cookie banners. Most notably, the DPA argues that all cookie banners must have a button within their first layer to reject all non-necessary cookies. This button must be as prominent as the button to accept all cookies. Furthermore, the DPA describes the criteria under which it considers the use of "cookie walls" ("pay or okay") to be permissible.	25 May 2022	FAQs (in German) Link
Austrian Federal Administrative Court: Media Privilege in Austrian Data Protection Act is unconstitutional; Constitutional Court to decide	The Austrian Federal Administrative Court ("**BVwG**") has filed an application to the Austrian Constitutional Court ("**VfGH**"), requesting it to repeal s9 of the Austrian Data Protection Act (DSG), which largely excludes media companies from the application of the Austrian Data Protection Act and the GDPR. The BVwG believes the provision violates the Austrian Constitution. This application was filed following an appeal by a complainant against a decision of the Austrian Data Protection Authority. The complainant had filed a complaint against the defendant media company. The media company had published a news story about a police raid in which illegal drugs had been found. In the article, a photo taken from the police file was published. In the photo personal data of the complainant, including his name, were visible, although the complainant had nothing to do with the police raid or the underlying criminal investigations. The Austrian DPA rejected the complaint, claiming that it was not competent for the complaint, as the Austrian Data Protection Act's media privilege automatically excludes all data processing by media companies for journalistic purposes from the scope of the Data Protection Act.	13 June 2022	Article (in German; the decision is not yet published) Link

Development	Summary	Date	Links
	Following an appeal against this decision, the BVwG has now requested the Constitutional Court repeal this broad media privilege as unconstitutional. The BVwG argues that it is (inter alia) a violation of the fundamental right to privacy and data protection that data processing by media companies for journalistic purposes is always and generally excluded from the applicability of data protection law. Instead, the BVwG argues, there should be a balancing of interests between the right to privacy and the freedom of the media. Furthermore, the BVwG considers the broad media privilege to violate Article 85 GDPR. The VfGH will now decide on whether to repeal this provision or not. Eversheds Sutherland Austria represents the complainant in this proceeding.		
Court of Audit Austria reviews Austria's National Cyber Security Coordination – finds several shortcomings	The Austrian Court of Audit (Rechnungshof) has audited the Austrian National Cybersecurity Coordination. It its audit report, it outlines several areas where further measures and improvements are recommended. Amongst other things, the drafting of better crisis management plans as well as the creation of a Cyber Rapid Response Team is recommended.	22 April 2022	Report (in German) Link
Austrian DPA prohibits controller's use of GPS tracking in company cars	In this case the controller had implemented GPS-tracking devices into its company cars for the purpose of easier administration of the use of the company cars. The controller claimed that this GPS tracking was justified by legitimate interest (Article 6 (1f) GDPR) as well as legal obligations under Labour Law to keep working time records. The DPA ruled that the processing could not be based on these lawful bases. While the DPA recognised that there was a legitimate interest in the use of GPS-trackers in company cars, it considered that this interest could be satisfied by less intrusive means. As such the processing was not necessary for this	22 April 2022	Link to summary of the decision (in German, in the DPA's newsletter) Link Need decision link

Development	Summary	Date	Links
	legitimate interest and Art. 6 (1f) GDPR had no valid basis. The same applied for the cited legal obligations, as these could be fulfilled by using less intrusive means as well. As the controller could not base the processing on any other legal basis, it was declared unlawful.		
Austrian Federal Administrative Court: Controller may no longer send newsletters to users who requested deletion of all their data	This case concerned a complaint against a controller who operates a news website. The complainant had subscribed to the controller's newsletter via their website, where he also had a user account. At some point, the complainant sent a general deletion request to the controller stating "Please delete all my data" (in German). The complainant did not use the unsubscribe link of the newsletter. Following this request, the controller deleted all data in the complainant's user account but did not unsubscribe him from their newsletter. Consequently, the controller sent ten further newsletter messages to the complainant. The complainant filed a complaint against this under the Austrian implementation of the ePrivacy Directive. The competent authority issued a fine to the controller amounting to €1,210 for sending direct marketing messages despite the user's request for deletion of data. The Federal Administrative Court affirmed this ruling. The Court stated that while the complainant had not specifically asked to be unsubscribed from the newsletter, a general request for deletion of all data implies both the request to be unsubscribed as well as a withdrawal of consent. Therefore, the controller should have also deleted the user's contact data processed for the newsletter. Furthermore, the newsletter is to be considered direct marketing under the ePrivacy Directive, as the newsletter invited its recipients to visit the controller's website and as such to visit the controller's (paid or advertisement-based) product. Sending such a newsletter is therefore only permissible under the requirements of the ePrivacy Directive and its Austrian implementation.	Date of Decision: 22 April 2022 Published: 8 April 2022	Decision (in German) Link

Austria

Development	Summary	Date	Links
Austrian Federal Administrative Court: Data about water usage of residential houses constitute personal data	The Federal Administrative Court ("**Court**") ruled on a complaint by a homeowner against its water supplier, claiming that the water supplier's automatic collection of data on the house's usage of water violated GDPR. The Court ruled that data on the water usage of (small) residential houses or flats constitutes personal data under GDPR, as it allows conclusions about the inhabitant's habits. However, the Court ruled that the operator was justified in processing this data in its legitimate interest under Article 6 (1,f) GDPR.	Date of Decision: 22 April 2022 Published: 8 April 2022	Decision (in German) Link
Austrian DPA: Ski lift operator may take and compare photos at lift access to prevent unauthorised transfers of personalized ski lift passes to other skiers	The complainant filed a complaint against the operator of a ski lift. Whenever a customer who had purchased a personalised ski pass passed the turnstiles to access certain ski lifts, the operator would automatically take a photo of the ski pass holder. This photo would then be compared (by an employee) to a reference photo taken when the turnstile was passed for the first time. The purpose of this is preventing unauthorised transfers of personalized ski passes. The customers were informed by signs about the taking of pictures. The complainant considered this a violation of GDPR, as he had not consented to this data processing. The DPA denied the complaint and considered the data processing to be compliant with GDPR. It ruled that the operator could rely on legitimate interest as a legal basis, as the processing of data was restricted to what was necessary, adequate, and proportionate. Furthermore, such systems are not unusual and are therefore to be expected by data subjects.	Date of Decision: 22 April 2022 Published: 13 April 2022	Decision (in German) Link
Austrian DPA: Individual subject to death threats can request search engine to remove link to contact details under right to be forgotten	The Austrian DPA decided upon a complaint against a search engine operator. The complainant had received death threats following certain politically controversial historical statements. The complainant	Date of Decision: 22 April 2022 Published: 26 April 2022	Decision (in German) Link

Development	Summary	Date	Links
	was a registered court expert and as such his contact details including his home address were publicly available in the official list of court experts which is published online. When the name of the complainant was entered into the search engine, the link to this entry and his home address could easily be found on the first page of the search results. The complainant requested that the search engine operator delete the link to this entry based on the right to erasure. The search engine operator refused, claiming that there was public interest in accessing the complainant's contact details as a court expert. The DPA ruled against the search engine operator and ordered it to delete the link to the entry. It considered that in this individual case, the interests of the complainant in his personal security clearly outweighed the operator's and the public's interest in keeping the link available. This was particularly the case, as anyone looking for a court expert would usually not do this via a search engine, but via the published official list of court experts.		
Austrian Federal Administrative Court: Credit agencies may process data on insolvency of data subjects for at least five years	A data subject who had been insolvent requested a credit agency to delete the data in respect of the insolvency under Article 17 GDPR. This request was denied by the credit agency, the Austrian DPA and, following an appeal, the Austrian Federal Administrative Court (the "**Court**"). The Court ruled that credit agencies have a legitimate interest in processing such data. To assess an appropriate storage period of such data, the Court referred to EU Regulation 575/2013. The Court deduced from this Regulation that such data may be processed by credit agencies for at least five years. As this period had not yet elapsed, the appeal was rejected.	Date of Decision: 22 April 2022 Published: 25 May 2022	Decision (in German) Link
Austrian DPA publishes new quarterly newsletter	The DPA's newsletter focusses on the implications of the planned "ID-Austria", an electronic means of identification under the EU eIDAS-Regulation.	22 April 2022	Newsletter (in German) Link

Belgium

Contributors

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

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

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

Development	Summary	Date	Links
The Belgian DPA fined an organisation who restored all personal data on a dismissed employee's work laptop.	On 1 April 2022, the Belgian Data Protection Authority (the "DPA") issued a fine of EUR 7,500 to an organisation who restored all personal data on an employee's work laptop after his dismissal. The organisation – acting as a data controller - breached Articles 5(1)(a) and 6(1)(f) GDPR as there was an absence of a legal basis for the processing of the employee's personal data and a denial of his rights (e.g. right to erasure, restriction of processing, etc.). Within its decision, the DPA explained that after a (one month) blocking period (having an automatic message warning to all subsequent correspondents that the person concerned is no longer performing his position within the company), the employer must delete the e-mail address when these constitute personal data. The dismissed employee must be able to take back or delete his private electronic communications before his departure. If part of the content of his mailbox must be recovered to ensure the proper functioning of the company, this must also be done before the employee's departure and in his presence. In the event of a contentious situation, the intervention of a confidential advisor is recommended. Furthermore, the consequences of dismissal should be regulated in an internal charter on the use of IT tools.	1 April 2022	Decision (French) Link

Development	Summary	Date	Links
	In addition, the former employer not only processed the data as a data controller, but also made use of a data processor with whom it had no data processing agreement. It was therefore also in breach of Article 28 GDPR.		
Temperature checks on passengers.	As part of the fight against COVID-19, Brussels Airport Zaventem and Brussels South Charleroi Airport carried out temperature checks on passengers from June 2020 until March 2021. Both airports used thermal cameras to check whether passengers had a temperature of above 38°C. In Brussels Airport Zaventem, those passengers with a temperature above 38°C needed to fill out a questionnaire relating to COVID-19-symptoms, which was carried out by the company 'Ambuce Rescue Team'. According to the strict interpretation by the DPA, the airports did not have a valid legal basis to process health data of their passengers. rocessing for reasons of public health or important public interest could only be relied upon as an exception pursuant to Article 9 GDPR, provided that it was based on a clear and precise legal standard and where the application is predictable for the data subjects. However, in this case, the temperature checks were based on a Protocol, which did not meet those requirements. Additonally, the DPA also found that the information obligation to the passengers and the quality of the data protection impact assessment was insufficient. Therefore, the DPA issued a fine of (i) EUR 200,000 to Brussels Airport Zaventem, (ii) EUR 100,000 to Brussels South Charleroi Airport and (iii) EUR 20,000 to Ambuce Rescue Team.	4 April 2022	Decision Brussels Airport Zaventem and Amuce Rescue Team (Dutch) Link Decision Brussels Airport Zaventem and Amuce Rescue Team (French) Link Decision Brussels South Charleroi Airport (Dutch) Link Decision Brussels South Charleroi Airport (French) Link
NMBS/SNCB fined after sending direct marketing e-mails.	The DPA issued a fine of EUR 10,000 to the National Railway Company of Belgium ("NMBS/SNCB") for sending a newsletter via e-mail to anyone who requested the free "Hello Belgium Railpass", without mentioning to the recipients how they could unsubscribe from it. The DPA ruled that the newsletter was a form of "direct	4 May 2022	Decision (Dutch) Link

Development	Summary	Date	Links
	marketing" as it provided commercial/promotional messages, such as hyperlinks to blogs on citytrip locations in Belgium. The NMBS/SNCB argued that the newsletter was instead necessary to guarantee the sanitary safety of the 3.6 million Belgian train passengers who requested the railpass "given the precarious situation in the second wave of the corona pandemic". Nevertheless, the DPA ruled that (i) the e-mail was not actually necessary to carry out the agreement between the NMBS/SNCB and the train passengers and thus, there was no legal basis for processing the personal data, and (ii) the practice was in breach of Article 21 GDPR, as the train passengers were unable to unsubscribe from the e-mail.		
Roularta and Rossel have been fined by the Belgian DPA in a large-scale investigation into cookies on press websites.	The DPA recently carried out a large-scale investigation on 20 Belgian news-websites in relation to their cookie banners. On 25 May 2022, a first fine of EUR 50,000 was imposed on the press group Roularta for managing cookies on the websites levif.be and knack.be. On 16 June 2022, the DPA imposed a second fine of EUR 50,000, but this time on the press group Rossel for incorrectly managing cookies on the websites lesoir.be, sudinfo.be and sudpressedigital.be. The DPA reminded us that persons responsible for websites that wish to place or read cookies on a user's device, must obtain the user's prior consent to do so, unless the cookies are strictly necessary (such as cookies for the proper technical functioning of a website). Statistical cookies are in principle not considered as strictly necessary. The consent for the processing of personal data through cookies on the websites levif.be and knack.be were not valid, because; (i) 60 (not strictly necessary) cookies were placed on the user's device before the user had given anyconsent, (ii) insufficient prior information about the cookies was given to the users, and (iii) the "consent-boxes" to install cookies by third parties were already ticked in advance. Moreover, consent could not be withdrawn as easily as it had been given.	Date of the Roularta Decision: 4 May 2022 Date of the Rossel Decision: 16 June 2022	Roularta Decision (Dutch) Link Rossel Decision (French) Link

Development	Summary	Date	Links
	In the case of the press group Rossel, similar breaches were established and found by the DPA.Additionally, Group Rossel's websites considered that "further browsing" was a sign of the user's consent, whereas, in order for consent to be valid, it must be the result of a clear and sufficiently specific active act. Group Rossel also incorrectly relied on 'legitimate interest' for placing analytical and social network cookies on devices, when they should have instead relied on 'consent'.		

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 61 37 1003
oliviachen@
eversheds-sutherland.com

Development	Summary	Date	Links
National Development and Reform Commission issues Several Opinions on Data Infrastructure System **《数据基础制度若干观点》**	On 21 March 2022, the National Development and Reform Commission issued the Several Opinions on Data Infrastructure System (the "Opinions"), for public comments until 5 April 2022. Intended to fully realise the value of data and promote the development of a digital economy, the Opinions consolidate the existing views of the public on the construction of a data-based system, data property rights, flowing transactions, income distribution, security governance and other institutional rules, and solicit further suggestions and opinions. An overview of the key points of the Opinions is as follows: • Data property rights: it is advisable to establish a modern data property rights system to promote orderly classification of ownership, use and other related data rights in order to meet the needs of data circulation and use. The data property rights system also intends to recognise and protect the legitimate rights and interests of all stakeholders in the data market, as well as define their rights and obligations. • The regulations in relation data flows shall be improved and standardised in order to build a trading system which	22 March 2022	

Development	Summary	Date	Links
	facilitates in-service circulation and supports both floor trading and over-the-counter transactions. • Income distribution of data elements: The market shall play a decisive role in resource allocation, whereas the government shall expand the scope of market-based allocation of data elements and participate in distribution channels based on value contribution, in order to improve the redistribution adjustment mechanism of data element income. • Security governance: There shall be a data governance mechanism in place with both an effective market and a promising government, constructing a multi-party collaborative governance model among the government, entities and society. The suggestions and opinions of the public will be taken into consideration in the subsequent policy formulation processes.		
Information Security Technology – Technical Specification for Caller Identity Authentication Using Crypto Tokens (Draft for Comments) **《信息安全技术** **基于密码令牌的主叫用户可信身份鉴别技术规范（征求意见稿）》**	On 30 March 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Technical Specification for Caller Identity Authentication Using Crypto Tokens (Draft for Comments) (the "Draft"), for public comments until 29 May 2022. The Draft set out the technical specifications for transmitting, verifying and displaying the trusted identity of the caller during communications based on the crypto token. It provides guidance on the design, production and testing of terminal systems which transmit, verify and display the trusted identity of callers, and could also be used for the design, development and testing of relevant operational service systems. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rules.	30 March 2022	
Information Security Technology – Security Capability Requirements for Big Data Services (Draft for Comments)	On 7 April 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Security Capability Requirements for Big Data Services (Draft for Comments) (the "Draft"), for public	7 April 2022	

Development	Summary	Date	Links
《信息安全技术 大数据服务安全能力要求（征求意见稿）》	comments until 6 June 2022. The Draft specifies the requirements for big data service providers in respect of organizational management security capabilities, security capabilities, data handling activities and specifically security capabilities of data service risk management. The details are summarised as follows: • Organizational management security capability: Big data security strategies and procedures shall be developed according to the requirements of the information security management system. The data security management system shall satisfy the compliance and risk management control requirements in relation to data security, in terms of the security management of big data service organisations and personnel and the data and system asset management. • Security capability of data handling activities: Data security protection measures for data collection, storage, use, processing, transmission, provisions, disclosure, destruction and other data processing activities shall be implemented from the big data platform and big data application business, in order to fulfil the data security protection requirements in relation to data processing activities for big data services. • Security capability of data service risk management: the security capability of data service risk management shall cover five aspects: risk identification, security protection, security monitoring, security response and security recovery. Risk response measures shall be undertaken to ensure data service and data assets are always under secure protection and to ensure the sustainability of big data service. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rules.		
Information Security Technology – Information Security Management	On 7 April 2022, the National Information Security Standardization Technical Committee issued the Information	7 April 2022	

Development	Summary	Date	Links
for Inter-sector and Inter-organizational Communications (Draft for Comments) **《信息安全技术** **行业间和组织间通信的信息安全管理（征求意见稿）》**	Security Technology – Information Security Management for Inter-sector and Inter-organizational Communications (Draft for Comments) (the "Draft"), for public comments until 6 June 2022. The Draft provides guidance on information security management systems ("ISMS") for inter-sector and inter-organisational communications, including but not limited to the following: • Information security strategy: The information sharing policy shall define how group members could collaborate in developing security management strategies and guidelines within the information sharing group, which shall be available to all group members involved in information sharing. • Information classification: Information shall be graded according to its legal requirements, value, credibility, priority, importance and sensitivity in respect of unauthorised disclosure or modification. • Information exchange security: In order to ensure full protection of information exchange within information sharing groups, the relevant details of the identifiable information source shall be removed when its anonymity is requested, and shared information shall be disseminated without disclosing the recipient's identity. • Control of malware: Information received from other group members shall be scanned for the presence of malware, regardless of whether there is scanning of intra-group communication. • Management of information security incidents: The group shall reach a consensus and publish guidelines for events of value to other group members, and group members shall only report potential incidents of value to other members. Information security incidents shall be investigated by the relevant group members or supporting members to minimize the risk of reoccurrence. • Business continuity management: The business continuity and disaster recovery plans developed shall meet the need to exchange sensitive information with group		

Development	Summary	Date	Links
	members in a secure manner, as part of the recovery process. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rules.		
Information Security Techniques – Guidelines for the Assessment of Information Security Controls **《信息安全技术** **信息安全控制评估指南（征求意见稿）》**	On 7 April 2022, the National Information Security Standardization Technical Committee issued the Information Security Techniques – Guidelines for the Assessment of Information Security Controls (the "Guidelines"), for public comments until 6 June 2022. The Guidelines provide guidance for reviewing and assessing the implementation and operation of information security control measures, including the technical assessment of information system control. The key aspects of the Guidelines are as follows: • Assessment process: Prior to the assessment, the appointed information security auditor shall be prepared to conduct control and testing. Each assessment item shall be prioritised based on risk, or be arranged according to the specific business processes or systems. When evaluating a single information security control measure, the auditor may first collect the preliminary information, review the planned work scope, liaise with the relevant contacts, conduct a risk assessment, and eventually prepare the assessment document as guidance for the actual assessment work. • Assessment methods: Auditors may adopt assessments such as process analysis, inspection, testing and validation, and sampling during the review of information security control measures. Testing and validation may require resource-intensive automated tools. The foregoing methods of assessment may be combined in use as appropriate, according to the nature of the assessment and the required assurance level. After taking into consideration the public opinions solicited, further adjustments may be made to the Guidelines in formulating the finalised rules.	7 April 2022	

Development	Summary	Date	Links
Circular on Launching the Campaign for "2022 Algorithmic Comprehensive Governance" **《关于开展"清朗·2022年算法综合治理"专项行动的通知》**	On 8 April 2022, the Office of the Central Cyberspace Affairs Commission (the "Office") issued the Circular on Launching the Campaign for "2022 Algorithmic Comprehensive Governance" (the "Circular"). The Circular details the focus areas of the underlying campaign, which promotes the implementation of the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (the "Provisions"). The Circular sets out the following five "key missions" of the campaign to strengthen the comprehensive management of Internet information service algorithms: • Self-inspection and self-correction: Guidance shall be provided to Internet enterprises to comprehensively sort out the application of algorithms according to the relevant requirements of the Provisions, conduct in-depth evaluation of algorithmic security capabilities, take active and effective measures to rectify issues of algorithmic applications, eliminate hidden dangers of algorithmic security and protect the legitimate rights and interests of Internet users. • On-site inspection: The Office takes the lead in forming a joint inspection team with relevant departments and local network information departments to conduct on-site inspections of Interpret enterprises in respect of their algorithm compliance and algorithm security capability. • Algorithm filing: The general principles, filing scope, filing requirements and consultation channels of Internet information service algorithm filing of the Provisions shall be interpreted and publicised to the enterprises. • Pushing primary responsibility: Enterprises shall be equipped with algorithm security governance institutions and specialised personnel appropriate for the business scale. They shall establish and improve their rules and regulations in relation to algorithmic security, actively make use of algorithmic services to spread positivity, dispose of illegal and indecent information, monitor	8 April 2022	

Development	Summary	Date	Links
	algorithmic abuse and disarrangement and avoid algorithmic security risks. • Timely issue rectification: In respect of problems identified during the inspection (e.g. imperfect measures, inadequate implementation, unsatisfactory results, etc.), timely rectification shall be made. Enterprises with illegal behaviors shall be held seriously accountable, punished and ordered to make rectifications pursuant to the Provisions. The campaign is ongoing and is expected to last until early December.		
Information Security Technology – Basic Requirements for Collecting Personal Information in Mobile Internet Applications **《信息安全技术移动互联网应用程序（App）收集个人信息基本要求》**	On 15 April 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Basic Requirements for Collecting Personal Information in Mobile Internet Applications (the "Requirements"). The Requirements provide guidance to app operators in regulating personal information collection activities, as well as to regulatory authorities and third party evaluation agencies in supervising, managing and evaluating application personal information collection activities. The Requirements divide the requirements for collecting personal information on mobile internet applications into aspects, including but not limited to: • Principle of minimum necessity: The collection of personal information shall be restricted to the minimum range necessary (inclusive of type, frequency, quantity, accuracy, etc.) for the processing purpose. The personal information shall be collected in a manner causing the least impact on personal information according to its sensitivity. • Collection of necessary personal information: Necessary personal information refers to the personal information necessary to ensure the normal operation of the basic business functions of mobile internet applications. The	15 April 2022	

Development	Summary	Date	Links
	personal information required shall not exceed the range of necessary personal information. • Full notification and effective consent: Certain notification and consent requirements shall be satisfied in respect of the basic business functions, necessary personal information, sensitive personal information and multiple service types. The consent to necessary and unnecessary personal information of applications shall be distinguished. • Collection and management by third parties: The collection of personal information by third-party applications accessed through the applications or third-party software development kits embedded in the applications shall be subject to security management. Additionally, Annex A of the Requirements stipulates the scope of necessary personal information and requirements of use for apps of common services types.		
Information Security Technology – Network Data Processing Security Requirements **《信息安全技术 网络数据处理安全要求》**	On 15 April 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Network Data Processing Security Requirements (the "Requirements"). The Requirements provide the general, technical and managerial requirements for network data processing security and the data processing security requirements in the event of a public health emergency. The key points of the Requirements are summarised as follows: • General requirements: It is essential to fully identify the data which requires protection in order to formulate a data security directory. The data shall be categorised and graded according to the actual circumstances of the network operator, subject to full compliance with laws and regulations. The security impacts and risks shall be analysed comprehensively, and effective measures shall be undertaken to ensure data security. A complete audit log shall be kept throughout the data processing process to ensure traceability of processing.	15 April 2022	

Development	Summary	Date	Links
	• Technical requirements: Certain technical data processing requirements are specified in respect of the collection, storage, use, processing, transmission, provision and disclosure of data. In terms of data collection in particular, security requirements for network operators collecting personal information have been set out, as well as details of the personal information security policy, the need to obtain the consent of the personal information subject and the prohibition of forced misleading collection. • Managerial requirements: Requirements related to the management of data processing security are outlined in respect of: (i) the person in charge of data security; (ii) the guarantee and assessment of human resources capability; and (iii) emergency management. • Public health emergency incidents: The Requirements further set out the data processing security requirements for Level I (particularly significant) and Level II (significant) response events. References are made to the personal information service agreement, personal information collection, face recognition and authentication.		
Information Security Technology – Risk Assessment Method for Information Security **《信息安全技术 信息安全风险评估方法》**	On 15 April 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Risk Assessment Method for Information Security (the "Method"). The Method, as a recommended national standard, provides guidance for information security risk assessments conducted by various organisations. The key aspects of the Method are summarised as follows: • Revision and improvement of requirements: The Method made revisions to: (i) the object, scope, implementation process and method of information security risk assessment; (ii) the methods of asset identification, threat identification and vulnerability identification; and (iii) the risk assessment method and calculation principle.	15 April 2022	

Development	Summary	Date	Links
	• Clarification of implementation key points of work forms of risk assessment: The Method outlines the basic concept, risk element relationships, risk analysis principle, risk assessment implementation process and assessment method. It further highlights the implementation key points and work forms of risk assessment throughout the information system life cycle. • Construction of risk assessment framework: The risk assessment framework shall be constructed in terms of three aspects: (i) the relationships among risk elements; (ii) the risk analysis principle; and (iii) the risk assessment process. • Formulation of implementation process and risk assessment method: The implementation process and method of risk assessment shall be formulated from the perspectives of assessment preparation, risk identification, risk analysis, risk assessment, communication and negotiation, and documentation.		
Network Security Standard Practice Guidelines - Information System Disaster Backup Practice Guidelines (Draft for Comments) **《网络安全标准实践指南—信息系统灾难备份实践指引（征求意见稿）》**	On 26 April 2022, the National Information Security Standardization Technical Committee issued the Network Security Standard Practice Guidelines - Information System Disaster Backup Practice Guidelines (Draft for Comments) (the "Draft"), for public comments until 10 May 2022. It provides guidance on how the security problems identified in cloud disaster backup applications could be solved, and facilitates the implementation of the Data Security Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China. The Draft addresses both the service provider and service recipient and sets out security measures for data security risks, personal information protection risks and security risks associated with new models (such as cloud disaster recovery), all in relation to demand analysis, function design and operational maintenance. The measures include but are not limited to the following: • Protection against data security risks: In terms of demand analysis, the service recipient shall conduct a	26 April 2022	

Development	Summary	Date	Links
	comprehensive analysis of the business and data of all information systems used or held by it, and understand the current status of general, important and core data processing. In terms of function design, the service recipient shall adopt a "two places and three centers" structure with cross-region deployment, independent data storage system and a business disaster recovery system for information systems which require high business continuity. In terms of operational maintenance, the service recipient shall formulate emergency plans for disaster recovery, conduct safety drills at least once annually and conduct regular training for personnel using the disaster backup system. • Protection against personal information risks: In terms of function design, the service provider shall design functions of synchronisation with the information system to query and delete personal information according to the relevant requirements of personal information security. In terms of operational maintenance, when the personal information is queried or deleted, the service recipient shall conduct a comprehensive analysis of the possible backups in the disaster backup system and conduct synchronous processing. • Protection against security risks associated with new models: In terms of demand analysis, the service recipient shall focus on analysing the security risks of entrusting others to design, operate and maintain the disaster backup system. If material risks are identified, the service recipient shall commence the relevant work. In terms of function design, the service recipient shall adopt a cloud-based disaster backup function design scheme for information systems which are less likely to suffer losses in the event of a disaster with relatively minimal potential losses. In terms of operational maintenance, in the event of a disaster, the service provider shall communicate the impact, response measures, recovery progress and other information with the service recipient in a timely, effective and accurate		

Development	Summary	Date	Links
	manner. Material incidents shall be reported to the relevant departments in time. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rules.		
Network Security Standard Practice Guidelines – Guidelines on Security Accreditation for Cross-border Processing of Personal Information **《网络安全标准实践指南一个人信息跨境处理活动安全认证规范》**	On 24 June 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 (the "Guidelines"). The Guidelines details the basic requirements for personal information protection accreditation, which is one of the four permitted mechanisms to satisfy the cross-border transfer requirements under Article 38 of the Personal Information Protection Law of the People's Republic of China. Despite the voluntary nature of accreditation for cross-border processing of personal information, the PRC government recommends parties seek accreditation by qualified entities. The Guidelines sets out the aspects which must be addressed to achieve accreditation, including but not limited to: • Entry into legally binding agreements: The parties (i.e., the domestic personal information processor and overseas personal information recipient) participating in cross-border transfer of personal information must enter into legally binding and enforceable documentation. This should specify that the overseas personal information recipient undertakes to comply with the unified personal information processing rules, be supervised by the accreditation institution and be governed by the applicable Chinese personal information protection laws and regulations, and shall identify the entity bearing legal responsibility in China, etc. • Security management of personal information within the organization: The Guidelines require each party to designate a Personal Information Protection Officer, who has sufficient knowledge of personal information	24 June 2022	https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf

Development	Summary	Date	Links
	protection requirements and appropriate experience and shall be a senior management-level employee within the organisation. Further, each party participating in the personal information cross-border processing activity must also establish a personal information protection unit. • PIPIAs: The domestic personal information processor must conduct personal information protection impact assessments ("PIPIAs"), which shall address whether the cross-border transfer complies with Chinese laws and regulations, the impacts of the transfer on the interests of the data subjects, in particular the impacts of the transfer on the legal environment of the foreign country/region and cybersecurity environment on the interests of data subjects, and other items necessary for protecting the rights and interests in relation to personal information. • Rights of the data subjects: In addition to obtaining accreditation of the cross-border transfer, the parties shall obtain the separate informed consent of the data subjects to the cross-border transfer of their personal information and shall facilitate the exercies of rights by the data subjects.		
Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification – Part 1: General Principle (Draft for Comments) **《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第1部分：总则（征求意见稿）》**	On 7 May 2022, the Department of Science and Technology, Ministry of Industry and Information Technology of the People's Republic of China issued the Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification (Draft for Comments) (the "Draft"), for public comments until 7 June 2022. The four industry standards (general rules, location, image file and SMS information) announced in the current Draft provide guidance on the collection and use of sensitive personal information in adhering to the principle of minimum necessity. Part 1: General Principle ("Part 1"), as one of the four industry standards, specifies the minimum necessary basic principles, assessment requirements, assessment methods and assessment	7 May 2022	

Development	Summary	Date	Links
	processes for the collection and use of personal information by apps. The key points of Part 1 are summarised as follows: • Principle of minimum necessity: Part 1 specifies the evaluation requirements for the minimum necessary principle in respect of collection and use of personal information by apps, outlining specifications for different dimensions of personal information processing (e.g. authority, notification and consent, collection, storage, processing, transmission, provision, publishing, deletion, etc.). • Basic assessment procedures: The procedure for application personal information collection and usage minimization and necessity evaluation shall primarily consist of five phases: (i) determining assessment objectives; (ii) selecting assessment indicators; (iii) formulating assessment plans; (iv) implementing assessments; and (v) deducing assessment conclusions. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rule.		
Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification – Part 2: Location (Draft for Comments) **《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第2部分：位置信息（征求意见稿）》**	As mentioned above, the Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification (Draft for Comments) provides four industry standards in respect of the collection and use of sensitive personal information in adhering to the principle of minimum necessity. Part 2: Location ("Part 2"), as one of the four industry standards, details the minimum necessary evaluation specifications for apps in processing the notification and consent, collection, storage, use and deletion of the user's personal information (location information). To facilitate the audience's understanding of the specifications, Part 2 further classifies the collectable location information by apps and sets out the typical application scenarios, which are summarised as follows: • Information classification: Part 2 categorises the location information data which could be collected by apps: (i)	7 May 2022	

Development	Summary	Date	Links
	terminal location information (e.g. satellite location information, wireless network information, mobile communication base station location, sensor and IP addresses, etc.); (ii) location information provided by the user; and (iii) location information embedded in image and video data. • Typical application scenarios: The location information collected is typically utilised in delivering services such as mapping, advertising, dispatching, asset management, searching, recommendation, portrait, etc.		
Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification – Part 3: Image File (Draft for Comments) **《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第3部分：图片信息（征求意见稿）》**	As mentioned above, the Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification (Draft for Comments) provides four industry standards in respect of the collection and use of sensitive personal information in adhering to the principle of minimum necessity. Part 3: Image File ("Part 3"), as one of the four industry standards, details the minimum necessary information and evaluation specifications for apps in the collection, storage, use, deletion and other activities related to personal information. To facilitate the audience's understanding of the specifications, Part 3 further classifies the collectable image file information by apps and sets out the typical application scenarios, which are summarised as follows: • Information classification: Images could be generated by photo-taking, screenshotting and reprocessing images. Based on the image content, the image information could be categorised into the following three types: (i) basic information, i.e. the basic feature information of an image, including its content information (original and encoded binary code), format, size and resolution; (ii) additional information which could be associated with the person, i.e. time the image was taken, photo-taking equipment, parameters, image name, etc.; and (iii) location information, i.e. the accurate location information when the picture was taken.	7 May 2022	

Development	Summary	Date	Links
	• Typical application scenarios: The image information collected is typically utilised in scenarios such as social networking, media publication, image processing, image recognition, cloud disk back-up and customer and after-sales services, etc.		
Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification – Part 11: SMS Information (Draft for Comments) **《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第11部分：短信信息（征求意见稿）》**	As mentioned above, the Application Personal Information Collection and Usage Minimization and Necessity Evaluation Specification (Draft for Comments) provides four industry standards in respect of the collection and use of sensitive personal information in adhering to the principle of minimum necessity. Part 11: SMS Information ("Part 11"), as one of the four industry standards, specifies the minimum necessary evaluation specifications for app access, collection, storage, use and deletion of users' mobile SMS (inclusive of MMS, 5G messages and other multimedia). To facilitate the audience's understanding of the specifications, Part 11 further classifies the collectable SMS information by apps and sets out the typical application scenarios, which are summarised as follows: • Information classification: Part 11 divides the information obtained in SMS messages into the following types: (i) local user identification, i.e. data for identifying or distinguishing the identity of the user of the mobile terminal where the SMS and MMS messages are located; (ii) end-to-end identification, i.e. data for identifying or distinguishing the SMS communication end-to-end identification information of the user of the mobile terminal where the SMS and MMS messages are located; (iii) SMS content, i.e. content in various forms which is edited by the SMS sender and sent to the recipient; and (iv) time, i.e. the time when the mobile terminal user receives or sends the message. • Typical application scenarios: The SMS information collected is typically utilised in scenarios such as SMS cloud back-up, easy access to verification codes, convenient SMS query and service subscription, optimisation of the editing and sending functions of SMS,	7 May 2022	

Development	Summary	Date	Links
	enhancement of SMS functions, data transmission between mobile phones, harassment interception, service intelligence, synchronisation or transfer of SMS across devices, equipment automation, archiving and equipment management by enterprises, on-board hands-free use and projection display, sending of emergency help SMS, local back-up and restoration of user data, etc.		
Classification Guide for Pre-installed Applications on Smartphones **《智能手机预装应用程序分类指南》**	On 9 May 2022, the National Information Security Standardization Technical Committee issued the Classification Guide for Pre-installed Applications on Smartphones (the "Guide"), which outlines the classification and requirements of pre-installed smart phone applications. The Guide applies to the production activities of smart phone manufacturers, and provides reference for supervisory management and testing assessment. Pre-installed applications on smartphones are categorized into (i) non-uninstallable and (ii) uninstallable pre-installed applications. Non-uninstallable pre-installed applications refer to the necessary applications for direct support of the operating system or realisation of the basic functions of smart phones. The functions of non-uninstallable pre-installed applications shall be limited to the following: system setting, file management, multimedia recording, dialing, sending and receiving SMS, address book, browser and app store. For pre-installed applications with identical functions, there shall only be one non-uninstallable pre-installed application.	9 May 2022	
Information Security Technology – Requirements of Privacy Policy of Internet Platforms, Products and Services (Draft for Comments) **《信息安全技术** **互联网平台及产品服务隐私协议要求（征求意见稿）》**	On 26 May 2022, the National Information Security Standardization Technical Committee issued the Information Security Technology – Requirements of Privacy Policy of Internet Platforms, Products and Services (Draft for Comments) (the "Draft") for public comments until 25 July 2022. The Draft details the requirements of privacy policies between providers and users of internet platforms, products and services. The key points of the Draft are summarised as follows:	26 May 2022	

Development	Summary	Date	Links
	• Scope: Privacy policies shall cover the applicable scope, summary, rules for collection and use of personal information, rules for ensuring personal information security, rules for protecting the rights of personal information subjects, rules for cross-border flow of personal information, rules for updating the privacy policy, etc.; • Publication and promotion: The Draft sets out rules which personal information handlers shall adhere to, including but not limited to (i) actively prompting the personal information subject to read the privacy policy prior to collection of personal information; (ii) the privacy policy shall be published on a page which is continuously and easily accessible to the personal information subject; and (iii) where multiple service types are involved in the products or services provided, the privacy policy shall only be used for the purpose of informing the personal information subjects of the general information processing situation, and no bundled consent to the personal information of the multiple service types shall be obtained at one time solely by requiring the personal information subject to agree to the privacy policy.		
Data Security Management Certification Implementation Regulations **《数据安全管理认证实施规则》**	On 5 June 2022, the State Administration for Market Regulation issued the Data Security Management Certification Implementation Regulations (the "Regulations"). The Regulations are formulated in accordance with the Regulations of the People's Republic of China on Certification and Accreditation. They stipulate the requirements for certification in respect of the collection, storage, use, processing, transmission, provision, disclosure and other processing activities involving the network data of network operators. Despite the voluntary nature of certification, network operators are encouraged to regulate data processing activities through certification and hence strengthen data security protection. Pursuant to the Regulations, the mode of data security management authentication shall consist of technical verification, on-site audit and post-certification supervision.	5 June 2022	

Development	Summary	Date	Links
	The certification process shall be divided into the following phases: • (i) certification entrustment, i.e. the entrusted agent shall submit the certification entrustment materials requested by the certification authority. The certification authority shall determine the certification scheme based on these materials; • (ii) technical verification, i.e. the technical verification authority shall conduct technical verification in accordance with the determined certification scheme and issue a verification report to the certification authority and entrusted agent; • (iii) on-site audit, i.e. the certification authority shall conduct an on-site audit and issue an audit report to the entrusted agent; • (iv) evaluation and approval of certification results, i.e. the certification authority shall make a certification decision based on the certification entrustment data, technical verification report, on-site audit report and other relevant information; and • (v) post-certification supervision, i.e. the certification authority shall regularly supervise the certified network operators within the validity period of certification. The certification certificate shall be valid for three years. Its validity shall be maintained through post-certification supervision by the certification authority. In the event the certified network operation no longer satisfies the certification requirements, the certification authority may suspend or revoke the certification certificate in a timely manner.		
Provisions on the Management of Internet User Account Information **《互联网用户账号信息管理规定》**	On 27 June 2022, the Cyberspace Administration of China issued the Provisions on the Management of the Internet User Account Information (the "Provisions"), which shall come into force on 1 August 2022. The Provisions are promulgated in order to regulate the management of information, in particular the management of	27 June 2022	

Development	Summary	Date	Links
	Internet user account names, to protect the legitimate rights and interests of citizens, legal persons and other organizations, to maintain a good network ecology and to create a clear and clean cyberspace. The key points of the Provisions are summarised as follows: • Registration and use of account information: Internet information service providers shall formulate and disclose the management rules and platform conventions of Internet user accounts, sign service agreements with Internet users and clarify the rights and obligations related to account information registration, use and management. The registration and use of account information of individual Internet users shall be consistent with the true information of the individual. The Provisions further detail the prohibited circumstances for registration and use of account information. • Account information management: Internet information service providers shall be primarily responsible for managing Internet user account information and equipping themselves with professionals and technical capabilities commensurate with the service scale. They are also responsible for establishing, improving and strictly implementing true identity information authentication, account information verification, information content security, ecological governance, emergency response, personal information protection, etc.		
Big Data Development Regulations of Sichuan Province (Draft for Comments) **《四川省大数据发展条例（草案征求意见稿）》**	On 23 March 2022, the Sichuan Provincial Department of Justice issued the Big Data Development Regulations of Sichuan Province (Draft for Comments) (the "Draft"), for public comments until 22 April 2022. The Draft is applicable to big data development and the relevant activities in Sichuan Province. By introducing specific requirements on the cultivation of data security awareness, security management, data classification, risk assessment, security measures and incident response system, the Draft aims to enhance the security of data and personal	23 March 2022	

Development	Summary	Date	Links
	information. The key points of the Draft are summarised as follows: • Cultivation of security awareness: The Draft advocates a culture of high data security awareness, which shall enhance data security protection capabilities, strengthen the construction of data security systems and maintain data security. • Security Management: The relevant cybersecurity and information department shall establish and strengthen the data classification and grading security system, in order to promote data security governance. The Provincial Big Data Center will be responsible for the promotion, guidance and coordination of the data security system construction. • Risk management: Local peoples' governments at all levels, as well as their departments, shall improve their risk assessment, monitoring, early warning and emergency response systems. The monitoring, early warning, control, emergency response and disaster recovery mechanisms for anti-attack, anti-leakage and anti-theft under the big data environment shall also be strengthened. The Draft also requires developing back-up capabilities to ensure data security during data collection, operation of shared applications and under open environment. After taking into consideration the public opinions solicited, further adjustments may be made to the Draft in formulating the finalised rules.		
Data Regulations of Chongqing **《重庆市数据条例》**	On 30 March 2022, the Standing Committee of the People's Congress of Chongqing Municipal voted to pass the Data Regulations of Chongqing (the "Regulations"). The Regulations provide that the processing of personal information shall adhere to the principles of legality, legitimacy and necessity. The Regulations provide specifications for data processing and security management in Chongqing, and shall come into force on 1 July 2022.	30 March 2022	

Development	Summary	Date	Links
	The Regulations set out the requirements in respect of, among others, data processing, data security, data resources and legal responsibility. Several key points addressed in the Regulations are summarised as follows: • Data security obligations: The Regulations have established and strengthened data processing and security rules and mechanisms under the Data Security Law of the People's Republic of China. In particular, it clarifies the data security obligations and specifies that the Municipality adopts a data security responsibility system in which each data processor shall be responsible for the security of its own data. It is specified that operators of online trading platforms shall be subject to obligations in respect of product and service quality assurance, consumer rights and interests protection, data and information security, labor rights and interests protection, fair competition, etc. • Management of data element market: Market entities shall not abuse their dominant market position by manipulating the market and setting forth exclusive co-operation terms. Data shall only be collected in a legal and legitimate manner, and such data obtained shall be utilised and processed in accordance with the law. Market entities shall obtain income from lawfully processed data products and services. • Legal responsibility in case of violation: Corrective measures or fines shall be imposed against parties which violate the open use agreement entered into with the Chongqing Big Data Development Bureau, fail to report data usage to the Bureau and use the public data beyond the agreed scope.		

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
2021 Annual report of the Office for Personal Data Protection published	On 11 April 2022, the Czech Office for Personal Data Protection has published their 2021 Annual Report. The report summarizes the Office's activity during the year 2021. In the report, the Office: • Stressed out the importance of observing the protection of personal data in relation to measures adopted because of the COVID-19 pandemic, as it is needed to both effectively use the citizen's personal data to combat the pandemic, but at the same time minimalize the impact on the citizen's privacy; • Provided an overview of the Office's inspection activity during 2021, both in connection with the COVID-19 pandemic and the standard agenda; and • Called for a stronger link between personal data protection and cybersecurity in the near future, given the omnipresent digitalization and associated risks of commercial misuse or hybrid warfare.	11 April 2022	Annual Report (Czech)
New reporting obligation for digital platform operators	In reaction to the DAC-7 EU Council directive, the Czech Parliament is currently discussing a legislation proposal, according to which digital platform operators would have new a reporting obligation about activities offered through digital platforms used for sale and provision of goods and services. Once a year, the operators would be obligated to submit electronic reports to the tax authorities regarding the revenue generated by users of these platforms.	14 April 2022	Legislative procedure progress overview at the Chamber of Deputies (Czech)

Development	Summary	Date	Links
	The obligation would cover four areas of activities: • provision of real estate (for housing or business); • provision of a means of transport (without a driver, as the provision of a transport service by a driver is a personal service); • personal service (i.e. work of a natural person based on time or task, both in online or physical environment); and • sale of goods (material goods and live animals); Operators would be obligated to collect certain personal data about the sellers who are individuals and inform them about the fact that such data are being collected. Furthermore, the operators would be obligated to evaluate the reliability of the provided personal data. In case of non-compliance of the operator with this reporting obligation, the platform may be blacklisted, resulting in operators being banned from making such platforms available to the sellers and sellers being prohibited from using the platform to provide goods or services. In case of non-compliance, even the seller as a natural person may be fined. The proposal is currently undergoing the legislative procedure and is subject to change.		
Whistleblowing directive transposition process continues; new draft law published	Czech Republic continues with the legislative transposition process of the EU Whistleblowing directive. The original legislative process was not completed before the December 2021 deadline and as a new government was formed, the process had to be restarted. A new draft has recently been presented to the government. The new draft limits the gold-plating of the previous proposal regarding the material and personal scope with changes such as: • reports on all administrative offences would no longer fall under the law, limiting the scope of the law only to offenses which bear the characteristics of a crime or a breach in 12 specific areas of EU law;	29 April 2022	Legislative documents (Czech)

Development	Summary	Date	Links
	• the general limit for employers from which the employer must implement an internal notification system has been increased from 25 employees to 50; and • a similar limit for the municipalities has been increased from 5,000 to 10,000 inhabitants. According to the legislative plan, the bill is expected to be voted on in September 2022, with expected effectiveness of the law on 1 July 2023.		

Germany

Contributors

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

Lutz Schreiber
Partner
T: +49 40 80 80 94 444
lutzschreiber@
eversheds-sutherland.com

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

Enrico Stuth
Trainee Solicitor

enricostuth@
eversheds-sutherland.com

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

Sara Apenburg
Senior Associate
T: +49 40 80 80 94 446
saraghoroghy@
eversheds-sutherland.com

Isabella Norbu
Associate
T: +49 89 54565 191
isabellanorbu@
eversheds-sutherland.com

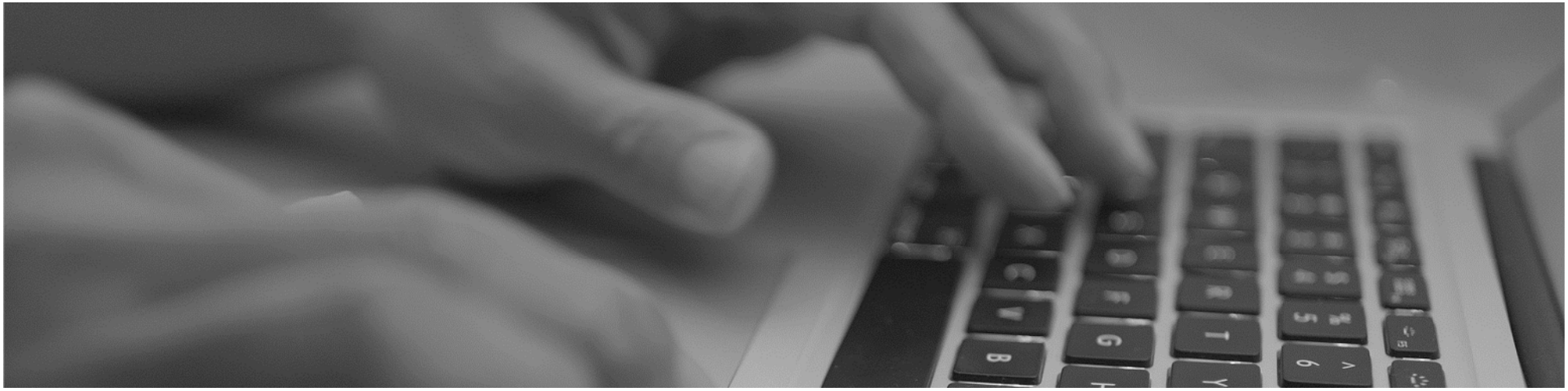
Jeanette da Costa Leite
Associate (PSL)
T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

Development	Summary	Date	Links
Supervisory Authority for Brandenburg and Baden-Württemberg stated that Cookie button options "accept all cookies" or "settings or refuse" are not sufficient	In its latest activity report for 2021, the Supervisory Authority for Brandenburg ("SA Brandenburg") reported that the cookie buttons "settings or refuse" do not fulfil the requirements for consent under of Article 7 GDPR. By using this cookie banner, the user cannot reject the cookies as quickly as they can accept them. To reject the cookies, the user must click on "settings" and then read through the settings too. The user is disadvantaged in their choice and therefore consent in the sense of Article 7 GDPR isn't freely given and is consequently invalid.	9 May 2022	Activity report 2021 (German only) Link

Development	Summary	Date	Links
	SA Brandenburg's activity report confirms the opinion of SA Baden-Württemberg in their FAQs about cookies and tracking from March 2022. In order to fulfil the consent requirements under Article 7 GDPR, cookie providers must provide the buttons "refuse all cookies" as well as "accept all cookies" on the same level and they should also add "settings" as a third option.		
Consumer protection associations can now also take legal action against personal data breaches	In its decision dated 28 April 2022, the European Court of Justice ("ECJ") has confirmed that consumer protection associations also have the right to sue if they intend to claim personal data breaches. Until now, this right wasonly possible for the data subjects themselves but from now on will also be possible irrespective of a specific damage event or instruction by the data subjects. According to the ECJ, the objective is to defend the interests of the general public against relevant breaches of data protection law. This puts the protection of the individual in the foreground, as intended by the GDPR.	28 April 2022	Decision (German) Link Decision (English) Link
What is the value of your personal data?	In some recent decisions the German courts have awarded compensation as damages underArticle 82 GDPR for minor data security breaches. In its decision dated 14 April 2022, the High Regional Court of Frankfurt am Main ("OLG Frankfurt a.M.") awarded €500 for a breach caused by a bank statement wrongly sent to a third party. For a data breach, where an unknown third party has obtained information in respect of ID , name and address, securities statements and tax, the District Court of Cologne ("LG Köln") has ordered an online broker service to pay €1,200 in compensation as damages. However, at the end of last year the District Court of Munich (LG München I) awarded €2,500 for the same type of data breach in another lawsuit.	Date of Decision (Frankfurt): 28 April 2022 Date of Decision (Köln): 18 May 2022	Decision OLG Frankfurt a.M. (German only) Link Decision LG Köln (German only) Link

Development	Summary	Date	Links
Supervisory Authority for Bavaria publishes guide on risk analysis	On 30th May 2022, the Supervisory Authority for Bavaria ("SA Bavaria") published a guide on risk analysis and Data Protection Impact Assessments (DPIA). It serves as an aid to detect and manage personal data risks more easily. The guide has practical tips for carrying out risk analysis, this includes a set of forms which are intended to guide the performance of risk analysis and support the development of proper documentation. The SA Bavaria plans to update this toolkit regularly.	30 May 2022	Press release (German only) Link Guidance from SA Bavaria (German only) Link
Data breach by the German Press Office?	The Federal Commissioner for Data Protection ("FCDP") sent a hearing letter to the federal press office in respect of the use of a social media page. According to a former expert's opinion, the German Press Office ("GPO") operating a "fanpage" on a social media network for the German Government page "Bundesregierung" does not comply with all requisite data protection laws. The hearing that is now underway is the first stage of the process. After reviewing the opinion of the GPO, the FCDP will decide whether administrative supervisory action is necessary.	3 June 2022	Press release (German only) Link Expert opinion (German only) Link
Supervisory Authority for Bavaria audits the IT security measures of Bavarian companies	The Supervisory Authority for Bavaria ("SA Bayern") wants to help Bavarian companies in fighting cybercrime. SA Bayern wants to comprehensively monitor the security of email accounts as a weak point of IT security. It also wants to review the IT security measures of Bavarian companies in order to improve those measures and each company's awareness of cybercrime. In the future, checklists on the most important areas of concern will be circulated.	2 June 2022	Press release (German only) Link
Health data collected because of Corona must be deleted	Many legal obligations that were related to the coronavirus pandemic have fallen away in the past few weeks. This also means that a lot of data processing operations are no longer necessary. The Supervisory Authority for Lower Saxony (SA Lower Saxony) therefore calls on companies to check what	19 April 2022	Press release (German only) Link

Development	Summary	Date	Links
	personal data (if any) they have collected and stored in connection with measures to combat the pandemic. If these measures have fallen away and with it the purpose for data processing operations, the data must be deleted.		
Top 10 cybersecurity threats for manufacturing and process automation systems	The Federal Office for Information Security published a list of the top ten cybersecurity threats and their countermeasures for manufacturing and process automation systems. Such systems are used in almost all infrastructures that handle physical processes. The basis for their evaluation is experience from previous security incidents, threats, feedback from the industry and it also includes the current new cybercrime trends. These new cybercrime trends include malware infections via the Internet and Intranet, software and hardware vulnerabilities in the supply chain and compromised extranet and cloud platforms.	31 May 2022	Press release (German) Link Press release (English) Link Industrial Control System Security (German) Link Industrial Control System Security (English) Link



Hong Kong

Contributors

John Siu
Partner
T: +852 2186 4954
johnsiu@
eversheds-sutherland.com

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

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

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

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

Justina Choi
Trainee Solicitor
justinachoi@
eversheds-sutherland.com

Hilary Chan
Trainee Solicitor
hilarychan@
eversheds-sutherland.com

Kevin Chan
Trainee Solicitor
kevinchan@
eversheds-sutherland.com

Development	Summary	Date	Links
PCPD issued guidance on recommended model clauses for cross-border transfers of personal data outside of Hong Kong	On 12 May 2022, the Office of the Privacy Commissioner for Personal Data ("PCPD") issued guidance on recommended model clauses for cross-border transfers of personal data outside of Hong Kong ("Guidance"). The Guidance contains two sets of recommended model contractual clauses ("RMCs") which may be incorporated into general commercial agreements between data transferors and recipients:	12 May 2022	PCPD Guidance Link

Development	Summary	Date	Links
	1. From one data user to another data user (i.e. data controller to data controller) in which the transferor and the transferee will both use the personal data for their separate business purposes (for example, as part of a data sharing collaboration for their respective business activities); and 2. From a data user to a data processor (i.e. data controller to data processor), which the transferee will only process the personal data for purposes designated by the transferor (for example, when a Hong Kong business enters into arrangements for an offshore cloud service). In summary: 1. The RMCs are recommended but not binding. Section 33 of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") which imposes restrictions on cross-border transfers of data is not yet in operation. 2. The Guidance is primarily prepared to assist local small and medium enterprises, but other corporations may take reference from the RMCs. 3. The RMCs can be used either where personal data is transferred by a Hong Kong entity outside of Hong Kong, or where personal data is transferred between entities outside Hong Kong, but such transfer is controlled by a Hong Kong data user. 4. The RMCs are prepared as free-standing clauses, which may be incorporated as part of general commercial agreements. 5. PCPD recommends that, in addition to the RMCs, data users may consider whether it is appropriate to incorporate additional contractual assurances set out in its earlier guidance issued in December 2014.		
PCPD laid charges in the first arrest case relating to doxxing	On 20 May 2022, the PCPD announced that it has laid four charges against an individual in respect of the disclosure of personal data without consent contrary to section 64(3A) of the PDPO, following the arrest of the relevant individual in December 2021. The purported disclosure of personal data arose from a monetary dispute between the relevant individual and the alleged victims. Under section 64(3B) of the PDPO, the individual may be liable	20 May 2022	PCPD Media Statement Link

Development	Summary	Date	Links
	for a fine of HKD100,000 and imprisonment for 2 years. These represent the first charges made in relation to doxxing since it was made a specific offence pursuant to the Personal Data (Privacy) (Amendment) Ordinance 2021, which came into effect in October 2021.		

Hungary

Contributors

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

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

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

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

Development	Summary	Date	Links
NAIH Resolution No 5255-2/2022 on the data protection requirements for drones intended for use by the Public Space Surveillance Agency	A municipal notary has requested that the Hungarian National Authority for Data Protection and Freedom of Information's ("**Authority**") opinion on the purchase of municipal drones to assist the work of the Municipal Police. Drones would be used for the following tasks: - detecting and documenting illegal dumping; - detecting areas infested with allergenic weeds; - quickly pinpointing the location of water accidents and incidents; - prevention and detection of poaching and unauthorised fishing; - detection of unauthorised construction activities; - surveillance of Natura 2000 areas, protected landscape areas and conservation areas to prevent the entry of quadbikes and dirtbikes/motorcross bikes. The Authority has drawn the muncipality's attention to the fact that if the data controller processes data that can be used to identify and recognise natural persons, the recordings constitute personal data and the person or body deciding to proceed with the camera processing is processing data.	20 May 2022	No link

Development	Summary	Date	Links
	The Authority stresses that it is not the use of drones per se that poses a data protection problem, but the atypical data processing, surveillance and image recording that can be carried out with the help of accessories mounted on to drones. The drone is untraceable and evasive, able to follow moving persons and objects without the knowledge of those involved. With this technology, the data controller can easily become capable of covert surveillance. The data subject's consent cannot be relied upon for such activity as the data subject is not in a real and free position to decide whether or not to be included in the drone footage. When recording with a drone-mounted camera, it is not possible to generally guarantee that exclusively the person concerned by the action of the Public Space Surveillance Agency is included in the recordings, and that no other person not concerned by the Public Space Surveillance Agency’s procedure or action is included at all. The Public Space Surveillance Agency may place a video recorder and record in a public place for public safety or crime prevention purposes in a way that is clearly visible to the public. However, in relation to this provision, it is important to point out that the drone is often undetectable and capable of rapidly changing position, in contrast to the static position of surveillance cameras and the highly visible nature of the recording device. In the case of a CCTV camera, people are well aware of the fact that there is camera surveillance in the area. When monitoring with a drone, there is no guarantee that the camera on the drone will only and exclusively monitor public areas. The Authority also draws attention to the fact that it is an offence to use an unmanned aerial vehicle over a residential area without authorisation or to make an unauthorised recording or recording of the sound or images of another person's home, other premises or fenced area when using an unmanned aerial vehicle without authorisation.		

Development	Summary	Date	Links
	To summarise, the Authority has drawn the muncipality's attention to the fact that in the case of law enforcement data processing in public areas by the Public Space Surveillance Agency, the processing of personal data that may be carried out by means of drone recordings cannot always be guaranteed to be lawful.		
Application of artificial intelligence to the analysis of customer service voice recordings (NAIH-7350/2021., NAIH-85/2022.)	A financial institution ("Bank") automatically analyses the recorded audio of customer service calls. The voice analytics software then ranks the calls based on this information, which categorises which person should be called back as a priority. This data is also stored in the voice analytics software linked to the call. The purpose of data processing is to monitor the quality of calls based on variable parameters, to prevent complaints and customer turnover and to increase the efficiency of call handling staff. The privacy statement on the Bank's website on the provision of telephone customer service to data subjects is general about this processing and does not contain any substantive information on voice analysis. The Bank's own data protection impact assessment concludes that the processing is high-risk for several reasons, that it is suitable for profiling or scoring and that the processing may have legal effects on data subjects. However, the impact assessment and the balancing of interests does not provide substantive solutions to address these risks. The Bank's statements also confirms that it is aware that it has not provided adequate information and the right to object for years in relation to the processing of the voice analysis under investigation, as it has decided that it is not feasible for it to do so. This contrasts with the Bank's privacy statement and its balancing of interests, which states that it fully guarantees the rights of data subjects. It expressly failed to consider the guarantee effect of the right to	20 May 2022	No link

Development	Summary	Date	Links
	adequate information and the right to object.As a result of the invalidity of the balancing of interests, the Authority is of the opinion that there is no legal basis in the GDPR for the automatic analysis of customer voice recordings as carried out by the Bank. In the context of the legitimate interest ground, it is important to stress that it is not intended to allow the controller to process personal data at any time and for any reason in the absence of other legal grounds. The safeguards should ensure, in practice, that the data subject is aware of the processing and can object to it, since theirright to object is exhausted once the processing has taken place. On the basis of the above, the Authority has found ex officio that the Bank's data processing practices in relation to the analysis of the audio recordings under investigation are in breach of the GDPR. The Authority has instructed the Bank to amend its data processing practices in order to comply with theGDPR, i.e. not to analyse emotions in the context of the voice analysis and to ensure that the data subject's rights in relation to the processing are adequately protected, in particular, but not limited to, the right to be informed and to object. In addition, the Authority imposed a sanction of a data protection fine of 250 million (Hungarian Forint) on the Bank.		

Ireland

Contributors

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

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

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

Development	Summary	Date	Links
The Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 (the "2022 Regulations")	The 2022 Regulations revoke and replace the Data Protection (Access Modification) (Health) Regulations 1989 (the "1989 Regulations"). This new legislation applies to organisations acting as controllers that process individuals' health data and receive data subject access requests from individuals set out in Article 15 of the General Data Protection Regulation (the "GDPR"). Under the 1989 Regulations, it was a mandatory requirement for any controller who was not a health service provider processing individuals' health data to consult with a health practitioner (e.g. a General Practitioner) before providing access to such data. Under the 2022 Regulations, it is at the controller's discretion when presented with a request whether to consult a health practitioner or not, subject to certain pre-conditions being satisfied.	15 March 2022	Regulation Link
The Director of Corporate Enforcement v DPC (Notice Party: Paul Coyle)	In 2020 the Data Protection Commission (the "DPC") upheld Mr. Coyle's complaint that the Director of Corporate Enforcement (the "ODCE") had unlawfully withheld access to Mr. Coyle's personal data relating to the liquidation of his business. The Decision found the ODCE refusal was contrary to the Data Protection Acts 1988-2003. In its appeal, the ODCE argued the DPC's Final Decision came to a different conclusion to that contained in the Draft Decision. The Director contends that the DPC did so without giving the parties fair notice of its proposal and without affording parties an opportunity to adduce evidence or make further submissions	1 April 2022	Decision Link

Development	Summary	Date	Links
	before the Final Decision was made. In April 2022, the Circuit Court found in favour of the ODCE's arguments and found the DPC's approach represented a fundamental departure from basic fairness of procedures in the decision making process. The Circuit Court has directed the DPC to reconsider the manner in which it had reached its final Decision.		
DPC publishes guidance for children on their data protection rights	The Data Protection Commission (the "DPC") has produced three short guides for children on data protection and their rights under the GDPR. These guides are aimed mainly at children aged 13 and over, as this is the age at which children can begin signing up for many forms of social media on their own. The protection of children's personal data is an important priority for the DPC, and is one of the five strategic goals of the 2022-2027 Regulatory Strategy published at the end of last year. The DPC published the following materials: Data protection - what's it all about? • This guide introduces children and young people to the idea of personal data and data protection, and why it is important for them to know about it. My data protection rights • This guide introduces children to the different data protection rights and how to use these rights. Top tips for keeping your data safe online • This guide has 15 useful tips to help children - and indeed everyone – for keeping their personal data safe online. The DPC has also produced a guidance note aimed at assisting parents/legal guardians in understanding the exercise of their children's data protection rights with entities and organisations in a variety of settings, such as schools, medical facilities or even play centres.	1 May 2022	DPC guidance note Link DPC guidance note Link

Development	Summary	Date	Links
	The DPC guidance note establishes a list of factors to be considered when exercising children's data protection rights, which includes; the age of the child, the nature of the personal data processed and whether the child would consent to the guardian exercising such rights.		
DPC issues guidance on the use of drones	Drones are becoming increasingly popular for both personal and professional use in Ireland. As drones are highly likely to capture the personal data of passers-by (data subjects) this may constitute personal data processing. In response, the Data Protection Commission (the "DPC") has issued guidance on the use of drones. These guidelines have been developed for drone operators for purposes other than public law-related purposes and also to answer queries from the perspective of data subjects. The DPC sets out the lawfulness of processing, the use of drones in the context of household or personal activity and the data protection obligations for data controllers as drone operators.	1 May 2022	DPC guidance note Link
DPC updates guidance for drivers on the use of dash cams	The use of dashboard-mounted video recording systems 'dash cams' has increased in recent years as devices have become more affordable and of higher quality. Where both video and/or audio of individuals in a vehicle (typically a taxi or bus) are recorded, or where video of a road user is captured by an outward-facing dash cam, data protection implications will arise and it is important that drivers who install dash cams understand their potential obligations under data protection law. The guidance sets out the controller's obligations, the use of dash cam footage and the sharing of such footage.	1 May 2022	DPC guidance note Link
DPC Inquiry into Pre-Hospital Emergency Care Council	The Data Protection Commission (the "DPC") commenced an inquiry to establish whether the Pre-Hospital Emergency Care Council (the "PHECC") was required to designate a data protection officer ("DPO") pursuant to Article 37(1) of the GDPR and whether the PHECC had done so. In addition, the Inquiry sought to establish whether the PHECC infringed Article 37(7) of the GDPR concerning the publication of the DPO contact details and the communication of this to the DPC.	3 May 2022	Decision Link

Development	Summary	Date	Links
	The inquiry was also commenced to establish whether the PHECC infringed Article 31 of the GDPR by failing to cooperate, on request, with the DPC in the performance of its tasks. The decision found that the PHECC had infringed Article 37(1), Article 37(7) and Article 31 of the GDPR. The decision noted that it cannot be the case that a public authority or body (or any controller), can fail to answer, in any way, repeated efforts to monitor and enforce the GDPR.		
Doolin v DPC (Notice Party: Our Lady's Hospice and Care Services) : New ruling from Court of Appeal on the use of CCTV footage	In Doolin v DPC (Notice Party: Our Lady's Hospice and Care Services), the Court of Appeal ("COA") examined the use by an employer of CCTV footage for disciplinary purposes. The COA upheld the previous High Court Decision and found the Data Protection Commission (the "DPC") had erred in law. The COA held it could not be said that Mr Doolin had either been notified that the CCTV may be used for disciplinary purposes or that there was any basis upon which he ought to have expected such use. The key takeaway: The judgment in Doolin is applicable to all processing of CCTV footage. As such, data controllers should reasonably ensure that data subjects, whose personal data may be captured by CCTV, are made aware of all purposes for which the CCTV footage may be used and that all policies are in place to reflect this.	24 May 2022	Decision Link

Netherlands

Contributors

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

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

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

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

Nathalie Djojokasiran
Junior Associate
nathaliedjojokasiran@
eversheds-sutherland.com

Ilham Ezzamouri
Junior Associate
ilhamezzamouri@
eversheds-sutherland.com

Natalia Toeajeva
Junior Associate
nataliatoeajeva@
eversheds-sutherland.com

Development	Summary	Date	Links
The District Court of Amsterdam rules that KLM is not allowed to ask candidate pilots about their COVID-19 vaccination status, as the request constitutes an unjustified infringement on the fundamental rights of candidate pilots.	The District Court of Amsterdam has recently ruled that asking job candidates (in this case candidate pilots for the company KLM) of their vaccination status is an unjustfied ingringement on fundamental rights. The preliminary relief proceedings took place between KLM (Royal Dutch Airlines) and the Dutch Airline Pilots Association ("VNV") who is a trade union that promotes the interests of candidates up for employment with KLM and pilots employed by KLM. On 10 March 2022, a candidate pilot sent an email to VNV stating that they felt compelled to take the COVID-19 ("Covid")	2 June 2022	ECLI:NL:RBAMS:2022:3029 Link

Development	Summary	Date	Links
	vaccination in order to get the job, and caused them mental problems. VNV argued that (1) KLM acted in violation of the GDPR and the Medical Examinations Act, and (2) KLM's actions made an unlawful distinction, on the basis of vaccination status between pilots already employed by KLM and pilots seeking employment with KLM. KLM argued that they wee allowed to impose the requirement of the disclosure of vaccination status in the recruitment process for applicants, as they will be deployed at all of the destinations in the KLM network and lack of knowledge regarding the pilot's vaccination statuscould have far reaching consequences for its business operations. KLM was also of the opinion that there was no form or intention of compulsory vaccination. As an employer, KLM argued that it was entitled to make requirements for its recruitment policy, in order to assess whether a candidate was fit for the job. The candidate however is free to determine whether he or she wishes to comply with those requirements. The District Court considered that the requirement of a vaccination against Covid constituted an unjustified infringement on the fundamental rights of candidate pilots, and in particular, infringed the privacy of article 8 of the ECHR. The Court therefore considered the following: (i) To ask for a vaccination is something that pre-eminently belongs to the private sphere. The requirement of a vaccination and the answer to the question of vaccination status is an infringement, and left candidate pilots of KLM with no choice in the matter. (ii) A breach could, under circumstances, be justified. To that end, the legitimate aim and appropriateness of the means of achieving that aim (and the proportionality and subsidiarity) would be examined. According to the District Court, KLM had not demonstrated that their interests relating to vaccination		

Development	Summary	Date	Links
	requirement was proportionate or that the intended purpose could not be achieved by other means. (iii) The VNV argued that there were alternatives to which candidate pilots and pilots in service were willing to participate, such as by taking PCR tests. Also, they identified that there may also be other reasons why pilots face travel restrictions besides Covid. VNV's claim to prohibit KLM from requesting candidate pilot vaccination status was therefore upheld.		
Dutch Data Protection Authority publishes year report on data breach notifications over 2021	On 25 May 2022, the Dutch Data Protection Authority ("DDPA") published its 2021 data breach report. In 2021, the DDPA received around 25.000 data breach notifications, which amounts to a rise of 4% in relation to 2020. The focus was mainly on cyberattacks and ransomware attacks on IT suppliers. In its report, the DDPA highlighted three types of cyber-attacks: hacking, malware and phishing. The DDPA noted that IT suppliers were increasingly targeted through cyberattacks, and were an interesting target for attacks because of the variety of services they provide and the large amount of personal data they accumulate. As organisations will often outsource their IT services to IT suppliers, IT suppliers are often acting as data processors. The final responsibility of compliance under articles 33 and 34 GDPR (regarding data breach notifications) ultimately lies with data controllers, and therefore it is for IT suppliers acting asdata processors, to communicate in a quick, transparent and complete manner to data controllers in cases of data breach. The DDPA found that IT suppliers often do not meet such requirements - for example,they often wait until an extensive investigation has been completed or are afraid of reputational damage. The DDPA however does not consider these to be valid reasons for delay.	25 May 2022	Report on data breach notifications 2021 (Dutch only) Link

Development	Summary	Date	Links
	The DDPA provided six (6) recommendations in itsreport: (i) Only engage with IT suppliers who provide sufficient guarantees for appropriate technical and organisational measures; (ii) apply data minimisation and monitor compliance; (iii) lay down concrete agreements in data processing agreements about the assistance of the IT supplier in any cases of data breach; (iv) periodically check the IT supplier's compliance with the processing agreement; (v) make a data breach notification action plan to meet deadlines; and (vi) make sure the data processing register has been (carefully) compiled. The DDPA also noted that some organisations do not inform data subjects that they have become the target of a ransomware attack. They instead often argue that they have instead paid a ransom, and believe that this was necessary / will stop the further distribution of personal data and notification is not required. However, the DDPA was of the opinion that payment of aransom was not an appropriate measure within the meaning of article 34 GDPR to not inform data subjects about the ransomware attack. The DDPA described Netherlands as in the top 3 countries with the highest number of data breach notifications. This is not surprising, since the Netherlands is highly digitized and thus the risk of data breaches is relatively high. Moreover, most data breach notifications came from the health and welfare sector (37%), followed by public administration (23%) and then		

Development	Summary	Date	Links
	financial services (11%), and that the most common type of data breach was when personal data was shared with a wrong recipient.		
GDPR limited by professional duty of confidentiality	In this recent casealaw firm, NautaDutilh, received a request to provide additional information regarding the personal data of the applicant in this case (whose information is omitted from the case decision). NautaDutilh took the position that it has provided the applicant with all the information that it was obliged to do so under Art. 13 GDPR (information obligation) and that a further provision of information could cause issues with the far-reaching duty of the confidentiality of lawyers. The District Court of Rotterdam followed NautaDutilh's reasoning, and stated that the GDPR's provision of information was not unlimited, and that the professional duty of confidentiality of a lawyer is a legitimate limitation to the duty to inform under the GDPR.	12 May 2022	ECLI:NL:RBROT:2020:13357 (Dutch only) Link
District Court of Midden-Nederland rules on the scope of right to access data (article 15 GDPR)	In this interim judgment from the Central Netherlands District Court, a data subject requested access to the processing of their personal data carried out by the defendant. The data subject wished to receive any and all information related to them , including any internal and external correspondence between employees, the defendant and third parties. The data subject also requested information relating to understanding what the data/information concerned, for example; what the purpose was for its use, to whom the data had been transferred, what safeguards were in place, information relating to the origin of the data, how long the data was to be stored, and whether automated decision-making (including profiling) was involved in the process. The defendant hadrejected the request of the applicant, but did provide an overview of the personal data of the applicant, which is covered by article 15 GDPR.	3 May 2022	ECLI:NL:RBMNE:2021:3243 (Dutch only) Link

Development	Summary	Date	Links
	The defendant was of the opinion that article 15 GDPR did not include a right to receive copies or access to the data directly, and cited that article 15 of the GDPR only entailed a right for the data subject to control if personal data concerning him or her was processed fairly and lawfully. As such, the defendant had therefore only provided the applicant with all data that had been processed by the defendant and which was covered by article 15 of the GDPR. In a renewed overview, the defendant did specify with which third parties it had exchanged personal data. Furthermore, an explanation was given for the purposes of understanding the processing of the data, the origin of the data, the categories of recipients, the potential transfers to third countriesetc. The District Court ruled that it followed from article 15 of the GDPR that the defendant did not have an obligation to provide the applicant with all documents containing personal data processed by the defendant. The defendant was instead allowed to limit itself to an overview of the personal data that it had processed of the applicant. However, this was only allowed in as far as the applicant, as data subject, and on the basis of the overview, was able to control the personal data that had been processed. Additionally, the District Court noted that there were exemptions to provide information, for example when it concerned information that should be used only for internal purposes, or where it concerned the personal thoughts of employees or legal analyses. The Court further considered that should a party argue that there should be more data provided, for example in this case the applicant, it must make a plausible case for such a request. The Court did however consider that the applicant had sufficiently proven that there may be more documents containing personal data related tothem, then as was initially stated in the overview provided by the defendant, and as such . The Court considered it important that the applicant had been involved in three complaint procedures and that these procedures did not appear in the		

Development	Summary	Date	Links
	overview. Although the defendant has chosen to only include personal data in the overview that fall within the scope of article 15 GPDR, the defendant was expected to give more detailed reasons as to how and why it concluded that the other data about the applicant did not fall under the right to access of article 15 GDPR. A general statement that certain documents are not covered by article 15 GDPR is insufficient. The defendant must now clarify and explain in more detail which documents contained personal data of the applicant, and to make it clear for each document whyit, or the personal data contained within it, did not fall within the scope of article 15 GDPR according to its opinion.		
The Dutch Data Protection Authority imposes highest fine to date on the Dutch Tax and Customs Administration for the violation of multiple GDPR principles.	The Dutch Data Protection Authority ("DDPA") has recently imposed the highest fine ever recorded to date against the Tax and Customs Administration ("TCA").. Following a recent investigation conducted by the DDPA into the Fraud Signalling Facility ("FSV")(in Dutch: Fraude Signalering Voorziening) application used by the TCA (which signals and records concerns for fraud and indicates a risk of tax and benefits fraud), the DDPA found that the TCA had violated the principles of data protection, by processing personal data in the FSV which was in violation of the principles of lawfulness, purpose specification, accuracy and storage limitation (article 5(1)(a) GDPR). In relation to these findings, the DDPA concluded the following: (i) There was no legal basis for processing personal data in the FSV application. The TCA had no legal obligation to signal fraud and information requests such as contra-information, andcould not rely onthe ground of 'necessary for the performance/task carried out in the public interest' to authorise the processing of personal data for supervisory purposes..	12 April 2022	Decision Fine DDPA (Dutch only) Link

Development	Summary	Date	Links
	(ii) The purposes for which the personal data was processed within the FSV application were not sufficiently specified. (iii) The personal data within the FSV was inaccurate and not up-to-date. Moreover, the TCA has not proven to have taken reasonable measures to rectify or erase personal data. (iv) The TCA had stored personal data longer than the retention period applicable.. **Absence of adequate technical and organisational measures** In addition to the violation of the aforementioned principles, the DDPA concluded that the TCA had not implemented adequate technical and organisational measures with regards to access control, logging, and/or logging controls, in order to guarantee an adequate level of security of personal data in the FSV application, and thereforeacted in violation of article 32(1) GDPR during the period between 4 November 2013 and 27 February 2020. **No proper and timely involvement of the DPO** Lastly, it was also found that the TCA had not properly or in a timely manner, involved the DPO in the implementation of the DPIA within the FSV application. This was therefore a violation of article 38(1) and article 35(2) GDPR. **Calculation of the fine** Within calculating an appropriate fine in this case, the DDPA considered the violations to be very serious and reflected within its final decision that the extent of the unlawful processing of personal data in the FSV application was severe due to impacting around 270,000 subjects across the span of approximately 6 years. The DDPA also considered the number of previous fines imposed against the TCA (approximately 3 in 3 years) in its final fine decision.		

Development	Summary	Date	Links
Ribank ordered to remove particularity codes from the Central Credit Information System	In this recent case from the Court of Amsterdam, an applicant was registered in the Central Credit Information System ("CKI") which includes a particularity code in respect of overdue loans with the defendant, Ribank. The applicant had repaid credit in full, and requested the removal of particularity codes in order to progress with the purchase of a house, and after weighing up the interests, the Court concluded that Ribank did have toremove the registrations. This was due to the fact that, at the time, the applicant had not been able to pay because theyhad travelled abroad to take care ofa sick parent, and furthermore whilst abroad, had spent some time in detention, so also further unable to make payments in a timely manner. After the detention, the applicant had made a payment arrangement with Ribank, which was fulfilled. The Court also ruled that the applicant's financial situation was stable, as they had several debts which had all been paid off, and also had athriving sushi business providing a stable income. The Court concluded that in its view of all of the above, and the applicant's financial stability, the applicant was unnecessarily restricted by the Credit Registration Office (BKR).	11 April 2022	ECLI:NL:RBAMS:2022:1224 (Dutch only) Link
The right of rectificationis only applicable to personal data if it concerns factual information	In this recent judgment from the Single Chamber, a claimant believed that a third party, Radboud University Medical Center (hereinafter "RUMC"), had included inaccurate and irrelevant personal data in the claimant's medical records. The claimant argued that the RUMC has wrongly rejected the claimant's request for rectification of such personal data, and that the DDPA (as defendant in this case) had wrongly refused to undertake any enforcement actions. According to the claimant, the collection and processing of the medical data concerned in this case, was notin compliance with the GDPR.	30 March 2022	ECLI:NL:RBDHA:2022:2432 (Dutch only) Link

Development	Summary	Date	Links
	In its findings, the Court declared the claimant's appeal as unfounded. The examples and statements of third parties, as provided by the claimant, did not contain any inaccuracies of factual information that could be easily and objectively established, and that the processing of the claimant's personal data was necessary for the performance of a treatment contract. Therefore, the DDPA held the view that the RUMC did not have to comply with the claimant's request for rectification. The Court stated in its decision that it had followed case law from the highest administrative court, in which the right to rectify personal data may only be exercised insofar as it concerns factual information/data. The right of rectification does not, in principle, apply to the reporting of impressions, assessments and conclusions. Furthermore, more recent case law shows that inaccuracies in personal data which needs to be rectified/corrected must be easily and objectively ascertainable.		
Dutch Data Protection Authority imposes a fine on the Ministry of Foreign Affairs - Violation of articles 32 GDPR (security of processing) and article 13(1)(e) GDPR (obligation to provide information regarding recipients or categories of personal data)	In this recent case, the Dutch Ministry of Foreign Affairs dealt with around 530.000 (Schengen) visa applications over the last year, all of which contained personal data (of the citizens applying for the visas) which was not handled and properly secured. As a result , it was found that the Ministry of Foreign Affairs hadacted in violation with article 32(1) GDPR and article 13(1)(e) GDPR. The personal data which was not properly secured concerned various types of data, including: fingerprint scans, names, addresses, places of residence, countries of birth, purpose of travel, nationalities and photographs. The application used by the Ministry of Foreign Affairs for visa applications is called the New Visa Information System (“NVIS”) (in Dutch: Nieuw Visum Informatie Systeem). The NVIS contains the application data of all applicants who want to obtain Shengen visas via a Dutch consular post abroad in order to obtain Shengen	9 March 2022	Decision fine DDPA (Dutch only) Link

Development	Summary	Date	Links
	visas for their stay in the Netherlands and/or in other Schengen countries. Data that is being processed in the NVIS qualifies as personal data, as referred to in article 4(1) GDPR, of which part of it is also considered biometric data under article 4(14) and article 9 GDPR, and as such are therefore special categories of data. Next to the GDPR, the following laws are important when it comes to visas: • The VIS Regulation This is important as it prescribes measures that should be implemented to physically protect data, including contingency plans for the physical infrastructure. • The BIO-standards These prescribe which targets should be met and how physical security can be ensured. **Security plan** Following information requests from the DDPA to the Minister of Foreign Affairs, as data controller, it has emerged that The Ministry does not have a security plan that meets the requirements of article 24 and 32(1) GDPR, as further elaborated in article 32(2) VIS Regulation and BIO-standards 5.1.1., 5.1.1.1. and 5.1.2.1. **Physical security** The Ministry failed to demonstrate that there were sufficient safeguards for physical security when working in NVIS in public places, and has not verified the effectiveness of the policy in this regard. The DDPA therefore concluded that there had been a violation of article 31 and 32 GDPR, as further elaborated in article 32(2)(a) and (k) of the VIS Regulation.		

Development	Summary	Date	Links
	Access rights Apart from the security issue, the DDPA requested from the Ministry the status of the set-up of access rights to NVIS and internal controls. Based on the documentation provided, the DDPA concluded that the Ministry did not have regular controls in place when it came to dealing with access rights, and certain employees were wrongly granted access rights. As such the DDPA concluded that the Ministry acted in violation of article 32 (1) GDPR, article 32(2)(f) and (k) VIS Regulation and BIO-standards 9.2.1., 9.2.2., 9.2.5. and 9.2.6, when it came to procedures regarding access rights in NVSIS. **Logging** With regards to the logging of files in the NVIS environment, the DDPA also noted that the Ministry did not have an adequate overview of the log files. Furthermore, these log files also showed inconsistencies in terms of their structure and the type of data they contained, and not all mandatory actions seem to be logged. Therefore the DDPA concluded that the Ministry did not regularly monitor the log files as there was actually no procedure in place for doing so, and that the Ministry therefore acted in violation of article 32(1) GDPR, article 32(2)(f)(i)(k) VIS Regulation and the BIO standards. **Security breaches** When it came to its judgment on security breaches, the DDPA concluded that the Ministry did not have an adequate procedure in place for security breach notifications, and that the Ministry had not taken sufficient and adequate organisational measures to prevent unlawful data processing in NVIS. As a result the Ministry violated the requirements laid down in Article 32(1) GDPR, article 32(2)(c)(d) VIS Regulation and the BIO standards 16.1.1. and 16.1.2.2.		

Development	Summary	Date	Links
	Information obligation Lastly, the DDPA noted that the Ministry mentioned only some categories of recipients, but not all. Following from article 13(1)(e) GDPR, a controller needs to inform data subjects about the recipients or categories of recipients of their personal data. It was therefore also found that the Ministry had therefore acted in violation of article 13(1)(e) FDPR and article 37(1)(c) VIS Regulation.		

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 Lada
Senior Associate
T: +48 22 50 50 734
piotr.lada@
eversheds-sutherland.pl

Development	Summary	Date	Links
Polish Voivodship Administrative Court in Warsaw: Each PESEL-related data breach must be assessed in the circumstances of the particular case	For years, the Polish Data Protection Authority has consistently recognized that PESEL number leakage poses a high risk to the rights and freedoms of individuals. PESEL (Universal Electronic System for Registration of the Population) is the national identification number used in Poland which identifies exactly one person and cannot be changed once assigned (among other things, it is used to identify oneself when dealing with authorities, in contracts or for medical services.) As a consequence, the Polish DPA considered that, in principle, each incident of a breach of personal data processing related to PESEL (e.g. its disclosure in e-mail correspondence) was reportable to the office, but also to the person to whom it belongs, and it affects the assessment of the breach itself, including the amount of the administrative fine. The case involved a relatively common breach, i.e., sending correspondence to the wrong addressee, while the unencrypted message contained the client's data such as name, postal code and PESEL number. The sender of such e-mail did not file a notification with the Polish DPA, believing that the risk associated with this data breach was not high and that it had taken sufficient	19 April 2022	Court Ruling (in Polish) Link

Development	Summary	Date	Links
	steps to prevent it (including collecting a statement from the recipient). The Polish DPA ruled that the sender was obliged both to notify it of the infringement and to provide such information to the customer whose personal data was sent to the wrong e-mail box, and imposed an administrative fine of PLN 160,000. The Voivodship Administrative Court in Warsaw overturned the administrative fine, stating that there had been a personal data breach which should have been reported to the Polish DPA. At the same time, the court held that the risk of violation of rights and freedoms was not high, and only at such a risk is the controller obliged to inform the personal data subject of the breach. Moreover, the court pointed out that just because someone obtains a PESEL number, even in combination with a first and last name or postal code, does not automatically pose a high risk to the data subject. In conclusion, it should be stressed that the risk assessment should be made taking into account the circumstances of a particular case, and breaches of confidentiality of personal data involving PESEL number, depending on these circumstances, may or may not result in a high risk of rights and freedoms of the personal data subject.		
Polish Data Protection Authority has clarified on responsibilities of Data Protection Officer	The Polish Data Protection Authority ("PDPA") issued the interpretation regarding the duties of the Data Protection Officer ("DPO"). According to the issued interpretation, if a controller, in performance of the obligations set forth in Article 29 and Article 32(1) and (4) of the GDPR, decides to use the measure of granting authorizations to process personal data by employees, it may authorize another person to grant authorizations to process data on its behalf, but this person should not be the DPO. This situation would lead to a conflict of interest because the DPO would be authorizing and then supervising and advising himself. The controller should appoint another person for this purpose, e.g. the head of the HR department or heads of other organizational units. Those persons can most precisely determine to whom and to what extent the authorization should be granted and update it on an ongoing basis.	10 May 2022	Statement (in Polish) Link

Development	Summary	Date	Links
	The DPO should not draft the data processing agreement. The PDPA emphasized that in such a case the DPO would first determine how the relationship between the controller and processor is to be shaped, as well as the rights and obligations of the parties to the agreement, and then, in performing its duties, would be required to assess the correctness and compliance of the decisions made in this regard. As a general conclusion, the PDPA noted that when shaping the scope of the DPO's duties, it is worth remembering that the DPO should not perform tasks that may subsequently become the subject of his or her monitoring activities or make decisions regarding the purposes and means of data processing and data security, as this would lead to a conflict of interest in this respect.		
Supreme Administrative Court: Ruling on Apostasy and the GDPR	The ruling by the Supreme Administrative Court ("SAC") concerned the relationship between the GDPR and the internal data processing regulations of the Catholic Church in Poland regarding the right to be forgotten after an act of apostasy. The judgment indicated that the Catholic Church may have different regulations regarding the right to be forgotten than the GDPR regulations. The SAC stated that the GDPR and the EU legislator intended to take into account the specificity of the processing of personal data related to religious practices and dogmatic teaching of churches and other religious communities. This is justified by the Constitution of the Republic of Poland and the Concordat with the Apostolic State and the principle of autonomy of the Catholic Church. The ruling of the SAC confirms the current practice of the Polish Data Protection Authority, which recognizes that it is not competent to handle complaints regarding the processing of personal data in church records, and the exclusive competence in this type of matters is vested in the Church Inspector of Data Protection.	25 May 2022	Court Ruling (in Polish) Link

Singapore

Contributors

Sze-Hui Goh
Partner

T: +65 8382 8702
sze-huigoh@
gtlaw-llc.com

Sharon Teo
Partner

T: + 65 9380 2637
sharonteo@
gtlaw-llc.com

Development	Summary	Date	Links
Launch of cybersecurity certification programme	The Cyber Security Agency of Singapore ("CSA") has launched a new cybersecurity certification programme, which provides recognition to enterprises that have adopted and implemented good cybersecurity practices. The certification programme comprises two cybersecurity marks: (a) Cyber Essentials – The Cyber Essentials mark is targeted at small and medium-sized enterprises ("SMEs") and provides recognition to SMEs that have implemented cyber hygiene measures. (b) Cyber Trust – The Cyber Trust mark is targeted at larger or more digitalised enterprises. It serves as a mark of distinction and provides recognition to enterprises which have implemented comprehensive cybersecurity measures and practices. The abovementioned cybersecurity marks certify the cybersecurity measures adopted by enterprises at the organisational level.	29 March 2022	CSA's press release Link Media factsheet regarding the Cyber Essentials and Cyber Trust marks Link
Establishment of the United States-Singapore cyber dialogue	Singapore and the United States have announced the establishment of the United States-Singapore Cyber Dialogue ("USSCD"). The USSCD will be held annually (or as determined by both countries) to further strengthen the cybersecurity cooperation between both countries.	30 March 2022	CSA's press release Link

Development	Summary	Date	Links
	Key features of the USSCD include the following: (a) Discussions between senior government officials from the cyber operational, technical, and policy units of various agencies on advancing practical bilateral cooperation; and (b) Discussions on areas such as the protection of critical information infrastructure, cybersecurity related to critical technologies, regional as well as international cyber policy, capacity-building, international standards and conformity assessment, countering ransomware and managing supply chain security.		
Publication of the guide to basic anonymisation	The Personal Data Protection Commission of Singapore has published a new Guide on Basic Anonymisation, which provides an introduction to basic anonymisation concepts and practical guidance on the anonymisation process, including how to appropriately perform basic anonymisation and de-identification of structured, textual and non-complex datasets.	31 March 2022	Guide to basic anonymisation Link
Launch of licensing framework for cybersecurity service providers	The CSA has announced the launch of its licensing framework for cybersecurity security providers ("CSPs") under Part 5 of the Cybersecurity Act 2018 ("CS Act"). The licensing framework is part of the CS Act and is targeted at protecting consumers' interests as well as improving the standards of CSPs. The CSA has also established the Cybersecurity Services Regulation Office to administer the licensing framework and facilitate liaisons with the industry and general public on licensing-related matters. Key features of the licensing framework are summarised as follows: (a) Types of licensable cybersecurity services: There are currently two types of licensable cybersecurity services under the Second Schedule of the CSA – (i) penetration testing services; and (ii) managed security operations centre monitoring services.	11 April 2022	CSA's press release Link Closing note to industry consultation on the licensing framework for cybersecurity service providers Link

Development	Summary	Date	Links
	(b) Main licensing requirements: Under Part 5 of the CS Act, there are two main requirements that CSPs must comply with: (i) ensuring that their key officers are fit and proper (i.e. any director or partner of the business entity or other person who is responsible for the management of the business entity) and (ii) keeping records of the cybersecurity services provided for a duration of at least three years. (c) Existing CSPs to apply for licence by 11 October 2022: Existing CSPs who are engaged in providing licensable cybersecurity services will have until 11 October 2022 to apply for a licence. CSPs who do not apply for a licence by 11 October 2022 will have to cease the provision of such services. For the avoidance of doubt, a CSP who applies for a licence by 11 October 2022 may continue with the provision of such services until a decision on their licence application has been made. Under the CS Act, any person who engages in the business of providing any licensable cybersecurity services to another person without a licence shall be guilty of an offence and liable on a conviction to a fine not exceeding 50,000 singapore dollars, or to imprisonment for a term not exceeding 2 years or to both. (d) Validity of license and fees: The validity of the license will be for a period of two years and the licence fees for individuals and businesses are 500 and 1,000 singapore dollars respectively. To support businesses due to the impact of Covid-19, a one-time 50% waiver of the licence fees will be granted for all licence applications that are lodged before 11 April 2023.		
Publication of the guidelines for critical information infrastructure owners to enhance cyber security for 5G use cases	The CSA has published the Guidelines for critical information infrastructure owners ("CII Owners") to enhance cyber security for 5G use cases (the "Guidelines"). The Guidelines set out measures to help CII Owners identify the potential threats that may be introduced to systems when they are connected to 5G services, and provide recommendations for mitigating cybersecurity risks. Using Microsoft's STRIDE threat model, the Guidelines identify the	29 April 2022	Guidelines for CII Owners to enhance cyber security for 5G use cases Link

Development	Summary	Date	Links
	following potential threats that may be introduced during connection to 5G services, and provide recommendations on how to mitigate each of the following threats: • Spoofing • Tampering • Repudiation • Information disclosure • Denial of Service • Elevation of Privilege		
Publication of the guide on responsible use of biometric data in security applications	The Personal Data Protection Commission of Singapore has published a new guide on the responsible use of biometric data in security applications, which is primarily targeted at applications that use biometric data (the "Guide"). The Guide is intended to help organisations to use security cameras and biometric recognition systems responsibly and safeguard individuals' biometric data where it is collected, used, or disclosed.	17 May 2022	Guide on responsible use of biometric data in security applications Link
Launch of National Integrated Centre for Evaluation	The CSA and Nanyang Technological University, Singapore ("NTU") have launched the National Integrated Centre for Evaluation ("NiCE"). The joint centre serves as a one-stop facility for manufacturers and developers to have their products tested and certified for cybersecurity robustness. NiCE will also contribute to research and development into advanced security evaluation techniques, such as those for software and hardware security protection. In addition to the above, NiCE will provide training and education to graduate students and industry professionals in relation to certification processes and evaluation methodologies.	18 May 2022	CSA's press release Link
Launch of AI Verify	The PDPC and the Infocomm Media Development Authority ("IMDA") have launched AI Verify, the world's first AI governance testing pilot framework and toolkit. AI Verify aims to help AI system-owners and/or developers test	25 May 2022	IMDA's press release Link MCI's press release Link

Development	Summary	Date	Links
	and verify the performance of their AI solutions through technical tests and process checks. It may be used by organisations who want to demonstrate to their stakeholders that their AI systems are accountable, transparent, safe and do not discriminate based on attributes such as race or gender. AI Verify is currently a minimum viable product. Singapore welcomes organisations from all around the world to participate in piloting the MVP and to contribute to building international standards in AI governance.		Invitation to Pilot Link
Launch of data anonymisation tool	The PDPC has launched a free to use data anonymisation tool. The data anonymisation tool will help organisations transform simple datasets by applying basic data anonymisation techniques.	30 May 2022	PDPC's infopage Link To download the anonymisation tool Link
The United Kingdom-Singapore Digital Economy Agreement Enters into Force	The United Kingdom-Singapore Digital Economy Agreement (the "UKSDEA") has come into force. The UKSDEA was signed between the UK and Singapore to establish digital trade rules and digital economy collaborations between the two countries.	14 June 2022	MCI's infopage Link MCI's press release Link

Spain

Contributors

Juan Díaz
Managing Partner
T: +34 91 429 43 33
jdiaz@
eversheds.es

Vincente Arias Máiz
Partner
T: +34 91 429 43 33
varias@
eversheds.es

Development	Summary	Date	Links
The Spanish Data Protection Agency ("AEPD") publishes a new section on its website which addresses processing of health data.	The AEPD has recently published a new section on its website which covers the issue of processing health-based data. The purpose of this section is to respond to calls from representatives of the health sector and user associations to have a compendium of legislation, criteria, doctrine and precedents in the field of health and data protection. The contents of this section are intended for citizens, data controllers, data protection professionals, health centers or the pharmaceutical industry, amongst others. The section is made up of seven sub-sections, which includes general information on the processing of health data and how to exercise the right of access to medical records, as well as questions related to medical research. It also includes the criteria set by the AEPD based on queries raised by the health sector, as well as information on files and ex-officio inspections. Additionally, the site coverstopics related to health research and clinical trials, as well as personal data breaches in the health sector. In the second half of 2021, 15% of notifications of breaches received by the AEPD were made by data controllers whose main activity sector was healthcare (i.e in the field of health).	4 May 2022	Direct access to the "Health" section in the AEPD website (in Spanish): Link
The Spanish Government passes the Royal Decree 311/2022, of May	The Spanish Government has recently passed the Royal Decree 311/2022.	3 May 2022	New National Security Scheme in the field of

Development	Summary	Date	Links
3, which updates the National Security Scheme in the field of Public Administration ("the New NSS").	This rule supersedes Royal Decree 3/2010, of January 8, which initially regulated the National Security Scheme ("NSS") in the field of Electronic Administration. The New NSS sets out the policy relating to security for the adequate protection of information processed and the services provided. The policy addresses this through reference to basic principles, minimum requirements, protection measures and compliance and monitoring mechanisms. The policy relates to bothpublic administration, as well as to technology providers from the private sector that collaborate with public administration. Key areas which the policy covers and the reason for the new update includes: (i) the adaptation of the former NSS to the new regulatory framework and the existing strategic context to guarantee security in the Digital Administration; (ii) the adjustment of the requirements to needs, groups of entities and technological fields for a more effective and efficient application; and (iii) updating the basic principles and security measures to facilitate a better response to new cybersecurity trends and needs. The New NSS seeks to guarantee the protection of information systems amongst the entities which fall within its scope of application, by reducing vulnerabilities and promoting continuous surveillance, establishing response mechanisms and by optimising security measures within the legal, technological, strategic and cyberthreat areas of the current framework.		Public Administration (in Spanish) Link
The Spanish Data Protection Agency ("AEPD") has issued a legal report which highlights the interaction between the Draft Royal Decree, GDPR and Spanish Data Protection Law.	The AEPD has recently published a report in which it discusses the correlation between the Royal Decree (however, this report is based on the preceeding draft of the finalised 311/2022 version), GDPR and Spanish Data Protection Law. This report is interesting because it shows the evolution from a personal data protection standpoint, the New NSS has undergone from its previous stage as a Draft Royal Decree in 2021. The report differentiates between the concept of "**information**	17 May 2022	Legal report 0064/2021 issued by the AEPD studying the interaction between the Draft Royal Decree which will regulate the new National Security Scheme, the GDPR and the Spanish Data Protection Act (in

Development	Summary	Date	Links
	security" (a set of techniques and measures aimed at guaranteeing the confidentiality, integrity and availability of information and important data for any organisation, regardless of their format) and the concept of "**personal data protection**" (a fundamental right for, of which the General Data Protection Regulation establishes a set of principles, rights, obligations and an organisational structure, with information security being one of the said obligations incumbent on data controllers and data processors). It also addresses the differentiation iproposed by the amendment of some wordings of the Draft Royal Decree, by considering the references it contains relating to personal data protection regulation are insufficient to guarantee adequate compliance. The report states that controllers and data processors must implement appropriate technical and organisational measures to guarantee a level of security adequate to the risk to the rights and freedoms of natural persons, but not exclusively limited to the security of said information, since personal data protection has a much broader scope. In this sense, personal data protection encompasses a much broader set of measures and guarantees, such as data protection policies, data protection by design and by default, or the notification and communication of data breaches.		Spanish) Link
The Ministry of Labour and Social Economy of Spain issues a guide covering existing obligations and rights in terms of algorithmic information in the Spanish legal-labour system.	The Ministry of Labor and Social Economy of Spain has recently issued a guide which covers the existing obligations and rights in terms of algorithmic information in the Spanish legal-labor system. All companies using algorithms or automated decision systems for an employee's management (i.e hiring, assigning tasks, productivity measurement, etc.) are subject to an algorithmic information obligation. The obligation of individual information is addressedin art. 22 of the GDPR. Within that section, it states that the use of such algorithm or automated systems must be carried out in a transparent manner, which is informative of the methods used and their specific purposes.	31 May 2022	Practical guide and tool on the business obligation to provide information regarding the use of algorithms in the workplace (in Spanish) Link

Development	Summary	Date	Links
	Therefore, it is also expected that someone explain the process to the employees using clear and plain language (and it is noted that it is not enough to just replicate the decision adopted by the algorithm). Similarly, any legal representation of staff must also be informed about how the use of said algorithms impacts decision-making, including profiling. The tool is divided into 4 sections (general information, information on the logic and operation, information on the consequences, and other relevant information), and each include different and relevant questions.		

United Kingdom

Contributors

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

Sarah Thorley
Associate
T: +44 1223 44 3782
sarahthorley@
eversheds-sutherland.com

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

Development	Summary	Date	Links
Court issues injunctions to deliver up or destroy confidential information following cyber attack	In Ince Group plc v Person(s) Unknown [2022] EWHC 808 (QB), an unknown defendant obtained confidential information about the claimant following a cyber-attack. A blackmail demand was made by the defendant with a threat to publish the stolen data on the dark web if a ransom were not paid. The judge was satisfied that the data in question attracted confidentiality and that the defendant could not rely upon the Human Rights Act 1998 with regard to freedom of expression. An interim prohibitory and mandatory injunction were granted requiring the delivery up and/or deletion and/or destruction of data it obtained. This case is another reminder to ensure you have appropriate security in place regarding your data and indicates the steps which are available at law when faced with a ransom demand.	1 April 2022	Link to case
High Court rejects Privacy International's judicial review claim in respect of bulk personal datasets	In R (on the application of Privacy International) v Investigatory Powers Tribunal and others the High Court considered whether a judicial review claim was permitted in respect of the sharing of bulk personal datasets ("BPDs") between UK and foreign intelligence agencies and whether the regulatory regime was compatible with Article 8 of the ECHR. BPDs contain personal data for individuals that are not necessarily the focus of intelligence investigations The case concerned an organisation challenging the tribunal's	4 April 2022	Link to Judgment

Development	Summary	Date	Links
	decision that the use of BPDs was compliant with Article 8 ECHR, specifically that the acquisition and use of such BPDs by intelligence agencies was compliant with Article 8 ECHR. The Court held that sharing BPDs would lead to interference with Article 8 ECHR rights and such sharing would therefore be unlawful unless captured by a justification under Article 8(2) ECHR. Dame Victoria Sharp P expanded that such a justification "requires that the interference is "in accordance with the law" and is necessary for, and proportionate to, a legitimate aim, here the interests of national security. The obligation for any interference with privacy rights to be in accordance with the law requires (a) a sufficient legal framework to regulate the interference, and (b) compliance with that framework." The Court held that on this basis the claim for judicial review was rejected as the Tribunal correctly identified measures necessary to comply with Article 8 ECHR and identified serious errors on the part of the agencies and noted that despite the errors the regime was compatible with Article 8 ECHR.		
DCMS issues a call for views in respect of strengthening the security of the UK data infrastructure industry.	The Department for Digital, Culture, Media & Sport ("DCMS") has issued a call for views on strengthening the cyber and physical security systems of the UK's data infrastructure industry. Specifically, the DCMS has requested views on tools used in other regulated sectors such as incident management plans in respect of UK data centres and online cloud platforms. The government intends to develop new protections for such infrastructure which will build on existing safeguards including the Networks and Information Systems (NIS) Regulations 2018 and seeks views from industry stakeholders to understand the risks data storage and processing services face. The call for views will also ask companies which run, purchase or rent any element of a data centre to provide details on their types of customers. The call for views will run until 24 July 2022 and responses will be used to determine whether the government needs to provide further support or management to minimise risk to data storage and processing infrastructure.	26 May 2022	Press release Call for views
High Court strikes out a misuse of private information claim in Smith and others v TalkTalk Telecom Group PLC	In Smith and others v TalkTalk Telecom Group PLC the High Court considered whether the claimant could successfully bring claims	1 June 2022	Judgment

Development	Summary	Date	Links
	for breach of the Data Protection Act 1998, misuse of private information. The case concerns an alleged mass data breach of data stored on the defendants servers which was allegedly obtained by criminal third parties and used for fraudulent purposes and unconfirmed breaches. Mr Justice Saini, delivering the judgment, has previously given the judgment in Warren v DSG Retail Limited which established that there must be some "positive act" to successfully establish a misuse of private information. The judgment therefore focused on whether this case was distinguished from the judgment in Warren or whether the decision was incorrect. It was accepted that the claim for breach of the Data Protection Act 1998 was legally viable. The defendant sought to strike out the claimant's application for misuse of private information (which was set out across several separate classes of claimants for separate breaches) and the claimant argued that the defendant has failed to adequately secure their data in a series of positive acts which made their data unsecure and therefore enabled third parties to access it. The claimant's sought to rely on an ICO decision which found the defendant had failed to put in place appropriate technical and organisational measures against unauthorised and unlawful processing of the personal data that could be accessed through the portal. The Commissioner found that the breach involved "multiple, systematic and serious" inadequacies by the Defendant to secure its systems. Mr Justice Saini decided that the misuse of private information claim was not viable following the rationale in Warren. He stated "the real complaint is not about misuse by the Defendants but about conduct which allowed others to misuse the Claimants' information. That is a matter for data protection law in the form of the DPA (or a claim for some other tort like negligence where protective duties are imposed). It is not within the scope of the tort of MPI.". The defendant had not themselves misused the private information and therefore the claim was not viable. The defendant also sought to strike out the unconfirmed breaches claim and the strike out application was dismissed on the basis that the breaches fell under the Data Protection Act 1998 and required that the claimants properly set out their claims in this respect.		

Development	Summary	Date	Links
Information Commissioner's blog highlights children's safety online and the work of the ICO internationally and publishes best interests of the child self-assessment tools and guidance	The UK Information Commissioner published a blog post on protecting children online. The blog post references the introduction of the ICO's Children's Code that came into force last year to help ensure children's safety online. It touches, however, on the fact that the value of the code would depend on its international reception, particularly due to the borderless nature of the digital world. The blog post highlights the actions of some other countries, whilst confirming that the Information Commissioner would be travelling to Washington in April to discuss the code with lawmakers, regulators and relevant companies. The ICO hope to continue to support developments that will further protect children in the UK, and view this work in Washington as an important part of this. The ICO has also published self-assessment tools and guidance to facilitate compliance with Standard 1 of the Children's code which requires online services to treat the best interest of children as a primary consideration when developing online services likely to be accessed by a child. The ICO's tools, templates and guidance focus on five key areas which are: • Best interests of the child overview • Understanding the rights of the child under the United Nations Convention on the Rights of the Child ("UNCRC") • Understanding the rights of the child under the UNCRC • Identifying potential impacts on the rights of the child in products or services • Assessing impacts on the rights of children and their likelihood and scale • Prioritising actions from risk assessments The four final points above form the basis of the self-assessment for organisations and the ICO provides template documentation to assist with self-assessments.	11 April 2022 27 April 2022	Blog post ICO guidance

Development	Summary	Date	Links
The Cabinet Office updates the Model Services Contract	The Cabinet Office has updated the Model Services Contract, a set of model terms and conditions for use by government bodies and other public sector organisations in relation to complex and high-risk services contracts with a total value over £20 million. The Cabinet Office have also published a list of the amendments, however the updates generally reflect changes in government policy, regulation and best practice. Some key updates include: • addition of Collaborative Working Principles; • addition of clauses concerning the supplier's compliance with Whistleblowing, Modern Slavery, Employment Law and Conflicts of Interest; • removal of the ability for authorities to enter into direct agreements with third parties that have more favourable terms than the supplier; • updated/deleted references to EU legislation such as GDPR provisions; • amendments to provisions on mandatory terms in subcontracts to recognise these may have been entered into prior to the main contract; • an increase to the suggested supplier liability cap for data protection breaches; • addition of references to Social Value requirements and KPIs or PIs; • updates security and encryption requirements for suppliers and subcontractors; • updates to the intellectual property rights provisions, which have been moved to a new Schedule; and • addition of new Financial Distress Events.	11 April 2022	Guidance List of changes Model Services Contract (Combined Schedules)
High Court dismisses claim against NHS Trust for misuse private information and breach of DPA 1998	In 2019, a 'pregnancy and parenting support club' named 'Bounty' were found to have unfairly processed personal data by the Information Commissioner's Office ("ICO") in breach of the Data Protection Act ("DPA") 1998 under Schedule 2. The ICO imposed a severe fine after investigating Bounty's data	19 April 2022	Judgment

Development	Summary	Date	Links
	processing activities whereby they failed to notify consumers that their information was/has been disclosed with third parties for direct marketing purposes, putting Bounty into administration. Hampshire Hospitals NHS Trust ("Trust") held a contractual arrangement with Bounty at the time, where Bounty permitted access to new mothers on Trust premises. The claimant and new mother, Mrs Underwood, claimed that Trust had misused her private information and breached the seventh data protection principle of failing to take appropriate measures to prevent unauthorised processing of her personal data. This claim was rejected by the judge holding that her personal data, found at the foot of her hospital bed, was necessary. Misuse of private information was also rejected by the judge as the information misused was obtained without Trust's consent, nor did it contain enough 'serious' data to relinquish its "trivial" attributes. For a claim to be: "actionable for misuse of personal information, the information must reach a level of seriousness before the tort is engaged". Exemplary damages were also dismissed as they are "wholly exceptional" and should not be added to a claim to "simply mark how upset the claimant is about the defendant's conduct, or as some sort of negotiating strategy".		
Improved AI and data protection risk toolkit finalised by the ICO	The ICO has launched an updated version of its AI toolkit which is designed to provide practical support to organisations to reduce the risks to individuals' rights and freedoms caused by use of AI systems. The toolkit divides the risks and controls by high-level lifecycles stages including business requirements and design, data acquisition and preparation, deployment and monitoring and training and testing to provide a guide as to what risks and controls individuals should consider when using AI systems. The toolkit further aligns risk assessment factors with relevant data protection legislation to enable individuals to comply with their legal obligations.	4 May 2022	Toolkit
The Queen's speech 2022	The Queen's Speech, delivered on 10 May 2022, announced the proposal to bring forward a Data Reform Bill (the "Bill") designed	10 May 2022	The Queen's speech

Development	Summary	Date	Links
announces Data Reform Bill	to reform the UK's data protection regime. The briefing notes that accompany the speech set out the purpose, main benefits and main elements of the Bill. The Bill is intended to ease burdens on businesses, boost the economy, and increase innovation by creating a new "trusted UK data protection framework", whilst also improving the lives of those in the UK. To reduce burdens on UK businesses, the Bill will create a more flexible framework that centres on privacy outcomes as opposed to a box ticking exercise, ultimately creating a greater culture of data protection. The briefing notes emphasise the impacts on scientific innovation, with hopes that simplified rules around research, along with clarifications on personal data use, will aid scientific and technological progress. The Bill also seeks to strengthen the powers of the Information Commissioner's Office whilst also ensuring its accountability to the public and to Parliament. It is hoped that the Bill will increase participation in smart data schemes to provide people with greater control over their data. The briefing notes also emphasise the effects the Bill is hoped to have on the delivery of services, particularly in relation to health and social care, security and government services, allowing public bodies to share data whilst providing a "gold standard" level of protection. The Bill will predominately apply across the UK, however some measures will apply to England and Wales only. Editors Note: the draft Bill was published on 18 July 2022. More to come in our next edition of UpData.		and briefing notes

United States

Contributors

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

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

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

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

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

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

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

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

Development	Summary	Date	Links
Connecticut passes new consumer privacy law, the CTDPA	Connecticut has implemented a new consumer privacy law, the "Act Concerning Personal Data Privacy and Online Monitoring" ("CTDPA") which is to take effect on 1 July 2023. The new law is applicable to business or persons that produce products or services for residents of Connecticut and control or process the personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data or those which controlled or processed the personal data of not less than 100,000 consumers excluding where such data is solely used to complete a payment transaction. However,	17 May 2022	Consumer privacy law Eversheds Sutherland International Alert

	the CTDPA does not apply to protected health information and other private information which is subject to specific federal laws. The CTDPA imposes an obligation on relevant businesses to provide consumers with a privacy notice if requested no later than 45 days following receipt of the request. The notice must contain specific data such as the categories of personal data processed by a controller, which categories of personal data are shared with third parties, how consumers can exercise their rights amongst other details. The controller must also describe one or more secure reliable means for consumers to submit requests to exercise their consumer rights. The CTDPA also requires that controllers and processors have a contract in respect of processing personal data. The contract must contain instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The processor must also ensure that those processing data under the contract are subject to a duty of confidentiality and that all data is deleted or returned to the controller at the controller's request at the end of the provision of services. The CTDPA also makes further provision for data security requirements to protect personal data, an appeals procedure for consumers in the event controllers refuse to take action on a request within a reasonable time which echoes data privacy legislation recently implemented in other US states such as Utah.		
FDA Issues Proposed Guidance on Medical Device Cybersecurity in the Health Care Sector	On April 8, 2022, the Food and Drug Administration (FDA) released draft guidance on a modernized framework for cybersecurity for medical device manufacturers and other stakeholders in the health care sector, particularly in light of the increasing use of wireless, internet- and network-connected devices, portable media, and the frequent electronic exchange of medical device-related health information. The guidance, titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," provides a modernized cybersecurity framework in response to increases in digital attacks targeting medical devices. It remained open for public comment through July 7, 2022, and would replace a previous framework established by the FDA in 2018. In the guidance, the FDA sets forth updated security principles for medical devices and promotes the use of Secure Product	8 April 2022	Text of Draft Guidance

	Development Frameworks (SPDFs) to mitigate the frequency and severity of cybersecurity incidents that threaten patient care. The guidance is most directly applicable to medical device manufacturers), but the cybersecurity implications are useful for other stakeholders like health care facilities, providers and patients who use or work with medical devices.		
FTC Chair Recommends New Approach to Data Privacy and Security Regulation	On April 11, 2022, Federal Trade Commission (FTC) Chairperson Lina Khan spoke at the International Association of Privacy Professionals' Global Privacy Summit in Washington, D.C., stating that the FTC should consider rethinking its traditional "notice and consent" approach to privacy regulation in the United States. She further noted that the Commission is well suited to tackle and appropriately police the new political economy of how companies collect and deploy data in America. At the summit she said, "(t)he general lack of legal limits on what types of information can be monetized has yielded a booming economy built around the buying and selling of this data," and noted that today's data practices create and exacerbate "deep asymmetries of information," further worsening the inequalities of power between businesses and consumers. Ms. Khan's statements suggest that the FTC may shift its approach to privacy regulation which could have a dramatic impact on certain types of business practices. As discussed further below, it is also worth noting that the Senate confirmed Alvaro M. Bedoya in May 2022, giving Chair Khan a 3-2 majority to pursue privacy reforms and enforcement actions without the need for bipartisan support. The FTC also changed its policies last summer to make it easier to bring investigative actions in certain areas, all of which indicates an impending wave of FTC investigations and enforcement actions.	11 April 2022	The Chair's Remarks
Colorado' AG Solicits Public Comments on Colorado Privacy Act Rulemaking	Colorado Attorney General Phil Weiser announced on April 12, 2022, that his office is soliciting informal comments from the public to facilitate a productive and effective formal rulemaking process. The Colorado Privacy Act was signed in to effect in July 2021, by Gov. Jared Polis, making Colorado the third state (after California and Virginia) to adopt a comprehensive privacy law.	12 April 2022	CPA Rulemaking Site Pre-Rulemaking Considerations for CPA Informal Comments Form

	As the state's attorney general, Weiser is responsible for the implementation and enforcement of the CPA and is charged with the adoption of new rules to effect the CPA by July 1, 2023. Mr. Weiser released the "Pre-Rulemaking Considerations for the Colorado Privacy Act" (the PRCs), providing guidance on key principles for the CPA rulemaking.		
DAO members may be jointly and severally liable for $55 million crypto theft resulting from a phishing attack.	On May 2, 2022, a putative class action was filed against a decentralized autonomous organization (DAO) and its members seeking to recover $55 million in cryptocurrency losses stolen during a hack into the DAO's decentralized finance (DeFi) platform. In November 2021, a bZx protocol developer fell victim to a phishing attack, and a hacker was able to access the private keys of those using the bZx protocol on Polygon and BSC with the developer's password. The hacker stole approximately $55 million in cryptocurrency. According to Plaintiffs, the hacker was able to take the funds because, at that time, only the operations on Ethereum were fully decentralized—BSC and Polygon "did not have the protection of the DAO." The putative class action claims Defendants were negligent by failing to maintain the security of funds deposited using the bZx protocol and supervise developers of and those working on the protocol. Plaintiffs aim to hold Defendants liable for the developer's negligence under a theory of respondeat superior. In this case, the DAO's members—some of whom may not have been involved in decisions allegedly resulting in the hack—are now exposed to liability due to the DAO's structure. It is important that those wishing to form a DAO carefully consider whether and where to obtain legal status, as the options and requirements vary by state (and country). However, irrespective of whether or where a DAO obtains legal status, it is important to note that whether a DAO registered in a particular state would maintain its legal status in other forums, such as in a US federal court case, is still unclear.	2 May 2022	Text of the Complaint
Biden Signs Better Cybercrime Metrics Act Signed Into Law	President Joe Biden signed the Better Cybercrime Metrics Act (BCMA) into law, on May 6, 2022, enacting the legislation proposed in response to increasing public concern about	6 May 2022	Text of BCMA

	cybercrime and the lack of comprehensive cybercrime data and monitoring in the United States. The BCMA requires the Department of Justice and law enforcement agencies to compile detailed cybercrime statistics and develop a taxonomy to help contextualize and sort cybercrime data. The new taxonomy may improve data collection on cybercrimes, assisting relevant stakeholders in performing risk assessments of certain categories of cybercrimes. The taxonomy is expected to be an important step in defining cybercrime metrics and providing recommendations to the DOJ and other authorities.		
New York Enacts Law Requiring Notice to Employees Regarding Electronic Monitoring	On May 7, 2022, an amendment to the New York Civil Rights Law (NYCRL) went into effect, requiring employers to provide notice to employees regarding electronic monitoring. New York state employers that monitor their employees' electronic communications are now required to provide written notice to new employees upon their hiring if the employer monitors or plans to monitor or intercept their telephone communications, email communications or internet usage. The amendment also requires that new employees acknowledge receipt of the notice. Under the amendment, employers are not required to obtain express acknowledgments from existing employees, but are required to post a notice in a "conspicuous place which is readily available for viewing" by existing employees subject to electronic monitoring.	7 May 2022	
FTC Adopts Policy Statement on 'Edtech' and COPPA	On May 19, 2022, the Federal Trade Commission (FTC) issued a new policy statement that underscored that edtech providers must fully comply with all of the provisions of COPPA and the COPPA Rule, and that such providers will be subject to the FTC's scrutiny. In particular, the FTC identified the following four areas of focus: Prohibition Against Mandatory Collection, Use Prohibitions, Retention Prohibitions, Security Requirements. Samuel Levine, director of the FTC's Bureau of Consumer Protection, noted that "students must be able to do their schoolwork without surveillance by companies looking to harvest their data to pad their bottom line," and "[p]arents should not	19 May 2022	Released Statement

	have to choose between their children's privacy and their participation in the digital classroom."		
FTC Confirms Alvaro Bedoya	Alvaro Bedoya was sworn in as a commissioner of the U.S. Federal Trade Commission (FTC) on May 16, 2022. Bedoya is well known in privacy circles, with his work focusing on the intersection of civil rights and digital technology and was particularly recognized for a report on the use of facial recognition technology by law enforcement. The long-awaited arrival of Commissioner Bedoya restores a Democratic majority that Chair Lina Khan lost in October 2021 when Commissioner Rohit Chopra left the FTC to lead the Consumer Financial Protection Bureau. With the support of Commissioner Bedoya and Democratic Commissioner Rebecca Kelly Slaughter, Chair Khan is expected to move forward now on an ambitious agenda. Areas in the privacy arena, where more activity is expected to be seen, include: Privacy, a.k.a. "Commercial Surveillance," Rulemaking, Privacy/Competition Intersection, Algorithmic Discrimination and Civil Rights Issues, and Health Information.	19 May 2022	
Supreme Court Reinstates Injunction Against Texas Social Media Law	In a 5-4 decision, the U.S. Supreme Court vacated the U.S. Court of Appeals for the Fifth Circuit's stay of a temporary injunction in NetChoice, LLC v. Paxton, a closely watched case involving a novel Texas law purporting to bar "social media platforms" from engaging in "viewpoint" discrimination. The May 31, 2022, ruling is a win for the world's largest online social media platforms as it reinstates a temporary injunction barring the Texas attorney general from enforcing the Texas law, known as H.B. 20. The decision does not prevent users from suing covered platforms under H.B. 20's private right of action. According to a press release from NetChoice following the Supreme Court's decision, the case will return to the district court for arguments on the merits. But how the Fifth Circuit responds to the Supreme Court's action remains to be seen.	31 May 2022	Text of HB 20

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:

- Sarah Thorley
- Rumaysah Khan
- Dave Hughes
- Lucy Wainman
- Oliva Carey
- Shanna Everson
- Thomas Elliott
- Joan Cuevas

eversheds-sutherland.com

© Eversheds Sutherland 2022. All rights reserved.

Eversheds Sutherland (International) LLP and Eversheds Sutherland (US) LLP are part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

This information is for guidance only and should not be regarded as a substitute for research or taking legal advice.

#201612698v4<Cloud_uk> - Updata Edition 16 - Master