EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

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

- developments regarding international data transfers, such as the new UK IDTA and Addendum to EU SCCs, and an announcement on an agreement in principle for a EU/US framework
- continued expansion of regulation on cybersecurity (for non personal data as well as personal data) carrying an increasing range of regulatory and reporting requirements eg the US Cyber Incident Reporting for Critical Infrastructure Act, new SEC proposals (here and here) and EU Data Act
- impacts emerging on a broader data governance horizon with new legislation to regulate activities online, meriting close attention including the Online Safety Bill (UK), Digital Services Act (EU)
- the lawful use of cookies, and analytics is getting significant attention across several countries, with important developments in Austria, Belgium (here and here) and the Czech Republic (here and here) amongst others
- ENISA and NIST have published several useful guides (including on the topic of implementing privacy and security by design) whilst several provincial authorities in China have been illuminating security expectations
- the Irish DPC and French CNIL have issued their reports during the last quarter highlighting the heightened scale of enforcement activity they are undertaking, common themes and their focus in the year ahead
- cloud service providers are likely to feel under closer scrutiny as the CNIL, Swedish and other authorities focus their attention on their activities. On a positive note, cloud infrastructure providers have been amongst the first to gain approval of a code of conduct from the CNIL

We hope you enjoy this edition of Updata.

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

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

Development	Summary	Date	Links
EDPB adopts opinion on whether data protection authority can order the erasure of personal data where request is not submitted by data subject	The European Data Protection Board ("**EDPB**") has adopted an opinion on whether Article 58(2)(g) GDPR could serve as a legal basis for a data protection authority to order *ex officio* (ie as a result of its office) the erasure of personal data, in a situation where such request was not submitted by the data subject. By way of background, Article 58 GDPR grants a number of investigative, corrective, authorisation and advisory powers to data protection authorities, to enable them to monitor the application of the GDPR effectively. Article 58(2)(g) empowers a supervisory authority to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19. The Hungarian data protection authority asked the EDPB to examine and issue an opinion on the application of Article 58(2)(g) as a legal basis for a data protection authority to order ex officio the erasure of unlawfully processed personal data, where the data subject has submitted no such request. The EDPB considered this question of interpretation as a "matter of general application" of the GDPR, which has the potential to infringe the fundamental right to data protection. The EDPB assessed whether Article 17 (the right to erasure) imposes an obligation to erase personal data on the controller only following a request from the data subject. It concluded that Article 17 provides for two separate cases for erasure that are independent from each other:	14 December 2021	Opinion

Development	Summary	Date	Links
	– the erasure at the request of the data subject – the erasure as a standalone obligation of the controller Accordingly, the EDPB found that Article 58(2)(g) **is** a valid legal basis for a data protection authority to order *ex officio* the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject. In addition, the EDPB clarified that the opinion does not assess the different powers listed in Article 58(2) GDPR, and their interplay. Therefore, the opinion is without prejudice to the other powers listed in Article 58(2) GDPR. In addition, this does not exclude the possibility for data protection authorities to base an order of erasure on another legal basis provided for in Article 58(2) GDPR. The opinion serves as a reminder that clients should be prepared to receive and respond to corrective orders from data protection authorities, including orders to erase personal data – even where this has not been specifically requested by a data subject.		
EDPB updates guidelines adopted at its December 2021 plenary on examples regarding personal data breach notification	The European Data Protection Board ("**EDPB**") has published an updated final version of Guidelines 01/2021 on Examples regarding Personal Breach Notification (adopted on 14 December 2021). The aim of the guidelines is to assist controllers to respond appropriately to personal data breaches and comply with their notification obligations under Articles 33 and 34 GDPR. Notably, the guidelines set out a number of examples of personal data breach incidents alongside recommended mitigation actions/steps to be taken in response to the incidents. Although, post-Brexit, EDPB guidelines no longer have direct relevance in the UK, the ICO has confirmed that these guidelines may provide useful guidance to UK organisations.	4 January 2022	Guidelines
EU GDPR code of conduct on clinical trials and pharmacovigilance reaches final stages of development	The European Federation of Pharmaceutical Industries and Associations has issued a statement on a GDPR code of conduct on clinical trials and pharmacovigilance, which has reached its final phase of review by data protection authorities before it is	13 January 2022	EFPIA statement

Development	Summary	Date	Links
	submitted to the EDPB for approval. The code was produced in light of concerns around the implementation of the EU GDPR in the health research space, and will enable the sector to align on "key data protection positions" providing greater clarity and more certainty for clinical research.		
EDPS opinion calls for ban of microtargeting for political purposes and prohibiting targeted advertising based on pervasive tracking	The European Data Protection Supervisor ("**EDPS**") has issued an opinion on the EU's proposed Regulation on transparency and targeting for political advertising, which lays down rules and obligations for providers of political advertising and related services to be more transparent in their use of targeting techniques. In the opinion, the EDPS welcomes the aim of the proposed Regulation and emphasises the need to complement the provisions applicable to the processing of personal data in the context of political advertising by going further and providing additional restrictions, including by (1) providing for a full ban of microtargeting for political purposes; and (2) introducing further restrictions of the categories of data that may be processed for the purposes of political advertising, including targeting and amplification, in particular prohibiting targeted advertising based on pervasive tracking.	20 January 2022	Press release Opinion Commission proposal on transparency and targeting of political advertising
European Parliament agrees on draft Digital Services Act	The European Parliament has agreed a draft Digital Services Act ("**DSA**"), which contains measures to tackle illegal content, ensure platforms are held accountable for their algorithms and improve content moderation. The draft was approved with 530 votes to 78, with 80 abstentions, meaning that negotiations may commence with French presidency of the Council, representing member states. The draft DSA defines clear responsibilities and accountability for providers of intermediary services and online platforms, including social media and marketplaces. Amongst other things, the DSA: – establishes a "notice and action" mechanism to enable the removal of illegal products, services or content online. On receipt of a notice, a provider of a hosting service will be expected to act "without undue delay"	20 January 2022	Press release

Development	Summary	Date	Links
	– provides stronger safeguards to ensure notices are processed in a non-discriminatory and non-arbitrary manner – applies specific obligations to very large online platforms to mitigate the risk they pose in relation to the dissemination of harmful and illegal content, including by way of mandatory risk assessments, risk mitigation measures, independent audits and the transparency of so-called "recommender systems" (algorithms that determine what users see) The European Parliament will now enter negotiations with the Council of the EU to reach an agreement on the draft DSA.		
ENISA reports on use of remote identity proofing and self-sovereign identity technologies	The European Union Agency for Cybersecurity ("**ENISA**") has published two new reports: (1) Remote Identity Proofing – Attacks and Countermeasures; and (2) Digital Identity: Leveraging the SSI Concept to Build Trust. ENISA stated that the reports support one of the key objectives of the EU regulation on electronic identification and trust services ("**eDIAS**"), to secure electronic identification and authentication in cross-borders online services offered within Member States, and will help shape the review of the eIDAS by the European Commission, including its European Digital Identity service proposals. The first report on "remote identity proofing", assesses what forms attacks take, for example, 3D mask attacks where 3D masks reproduce the real traits of a human face and deepfake attacks using software create synthetic video footage or imagery representing someone else; and how measures can be introduced to combat them, for example, by setting video quality minimum settings, better identity document data controls and checking user face depth as well on a scan. The second report discusses self-sovereign identity technologies, which aim to give identity holders greater control over their identity. The report covers possible architectural elements and mechanisms of governance, and identifies security risks and opportunities with the aim to achieve the objectives set by the eIDAS Regulation.	20 January 2022	Press release Remote Identity Proofing - Attacks & Countermeasures Report Digital Identity: Leveraging the SSI Concept to Build Trust Report

General EU and International

Development	Summary	Date	Links
ENISA publishes report on data protection engineering	ENISA has published a new report on data protection engineering. The report takes a "broader look into data protection engineering to support practitioners and organisations". In doing this, the report aims to help practitioners and organisations with the practical implementation of technical aspects of data protection by design and by default. The report also acknowledges that new models of data processing introduce new threats and challenges, including lack of control and transparency, automated decision making and profiling, which need to be managed. The report considers security technologies and techniques, analysing their strengths and applicability to meet data protection requirements under Article 5 of the GDPR. This includes the consideration of mechanisms such as: anonymisation, privacy preserving computations, storage, transparency and user control tools. As part of this analysis, the report assesses the most relevant techniques depending on each processing operation and on the need of the controller. It also seeks to discuss both traditional security techniques, such as access control and privacy preserving storage, alongside novel concepts such as synthetic data. ENISA has also set up an Ad Hoc Working Group on Data Protection Engineering, which will be open until 15 February 202022. The working group's role is to analyse available and emerging technologies and techniques with the goal of identifying "good practices and innovative security techniques".	27 January 2022	Press release Report Working group
European Parliament publishes infographic highlighting the main emerging threats to Cybersecurity in 2021	The European Parliament has published an infographic on the main and emerging threats to Cybersecurity in 2021, resulting from, at least in part, digital transformation and Cybercriminals taking advantage of the COVID-19 pandemic. The European Parliament identified the following sectors as being the most affected by cybersecurity threats from April 2020 to July 2021: – Public administration/government (198 threats) – Digital service providers (152 threats) – General public (151 threats)	27 January 2022	News

Development	Summary	Date	Links
	– Healthcare/medical (143 threats) – Finance/banking (97 threats) They also identified the following as the nine prime threat groups: ransomware; cryptojacking; treats against data; malware; disinformation/misinformation; non-malicious threats' threats against availability and integrity; email-related threats; and supply chain threats. Ransomware, where attackers encrypt an organisation's data and require payment to restore access, was highlighted as the most worrying threat. In 2021 a corporate ransomware attack occurred every 11 seconds. Further, according to data from the EU Agency for Cybersecurity, the highest ransomware demand grew from EUR 13 million in 2018 to EUR 62 million in 2021, with the average ransomware pay doubling from EUR 71,000 in 2019 to EUR 150,000 in 2020.		
EDPB releases draft guidelines on right of access for consultation	The EDPB published its draft Guidelines 01/2022 on data subject rights - Right of access, for public consultation. The guidelines set out the aim and overall structure of the right to access, as provided for under Article 8 of the EU Charter of Fundamental rights and Article 15 of the EU GDPR, as well as the scope of the right to access, how to provide access, and the relevant limits and restrictions, amongst other things. The consultation closed on 11 March 2022.	18 January 2022	Guidelines Press release Consultation form
First code of conduct for data protection in cloud infrastructure is launched	Following approval being granted by the EDPB and CNIL, the Cloud Infrastructure Service Providers in Europe (CISPE) Code of conduct for Data Protection in Cloud Infrastructure has 'gone live'; the first group of members have declared that their services are compliant with the Code. The code is the first GDPR code of conduct that has been designed specifically for cloud infrastructure service providers.	3 February 2022	Press release Code
ENISA and CERT-EU publish 'Boosting your Organisation's Cyber Resilience' report	The ENISA and CERT-EU have published a joint report detailing best practices for public and private organisations in the EU as a result of a continuing rise in cyber-security threats. ENISA and CERT-EU have set out 14 best practice points, but note that "they	15 February 2022	Boosting your Organisation's Cyber Resilience Report

Development	Summary	Date	Links
	are provided in no particular order … organisations should prioritise their actions according to their specific business needs". – Ensure remotely accessible services require multi-factor authentication – Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application – Ensure all software is up-to-date – Tightly control third party access to your internal networks and systems – Pay special attention to hardening your cloud environments – Review your data backup strategy – Change all default credentials and disable protocols that do not support multi-factor authentication or use weak authentication – Employ appropriate network segmentation and restrictions to limit access and utilise additional attributes when making access decisions – Conduct regular training – Create a resilient email security environment – Organise regular cyber awareness events – Protect your web assets from denial-of-service attacks – Block or severely limit internet access for servers – Make sure you have the procedures to reach out and swiftly communicate with your CSIRT		
The new EU Data Act: European Commission proposes measures for a fair and innovative data economy	On 23 February 2022, the European Commission announced a new addition to its digital rulebook in the form of a proposal for a new Data Act, and accompanying sector-specific regulations. The proposal has significant implications for both holders and users of data (whether personal data or otherwise). Accordingly, the scope of the Act goes far beyond the boundaries of GDPR.	23 February 2022	ES briefing on the Data Act

Development	Summary	Date	Links
	These proposed rules will set out who can use and access data generated by connected devices, primarily in relation to industrial data, across all economic sectors in the EU. It forms part of the Commission's wider Data Strategy which focuses on ideas and actions to enable digital transformation (and is also closely linked to the wider EU Industrial Strategy). The Data Act is the second proposal, alongside the Data Governance Act, aimed at making the EU a leader in the data-sharing space. As part of this, the EU has new initiatives on an EU federated cloud, an industry alliance for cloud architectures, and is seeking to create both a horizontal and vertical ie sector specific data segments. Together, these proposals are intended to "unlock the economic and societal potential of data and technologies" and create a single market for the free flow of data the EU. This Data Act looks to harness the potential power which data has as a "non-rival good", which means that it can be used at the same time by many individuals, and consumed over and over again without impacting the quality of the data or depleting the supply. This contributes to the value of data, which has broad benefits; according to the Commission, however, only 20% of industrial data which exists in the EU is currently used. The Data Act, therefore, hopes to remedy the perceived under-use of data by providing new rules to make data available for reuse, and to address the legal, economic and technical barriers that currently exist and reduce data use. Read our briefing for further information on the Data Act.		
European Commission seeks feedback on Data Act proposals	Further to releasing details of a Proposal for a Regulation on harmonised rules on fair access to and use of data (**Data Act**) in February, the European Commission is calling for feedback on the proposals which will be summarised and presented to the European Parliament and Council with the aim of feeding into the legislative debate. The deadline for providing feedback is 13 May 2022. See our briefing for further information on the Data Act.	14 March 2022	Data Act proposal Call for feedback ES briefing on the Data Act

General EU and International

Development	Summary	Date	Links
EDPB releases new resources following March plenary	Following its March 2022 plenary, the European Data Protection Board has released the following resources: – Guidelines 02/2022 on the application of Article 60 GDPR – to promote the consistent application of the legal provisions relating to the one-stop-shop mechanism and to help supervisory authorities interpret and apply their own national procedures in alignment with the one-stop-shop mechanism – Guidelines 3/2022 on Dark patterns in social media platform interfaces – providing practical recommendations to designers and users of social media platforms on how to identify and avoid "dark patterns" in social media interfaces (ie interfaces presented by social media that cause users to make unintended, unwilling and potentially harmful decisions regarding the processing of their personal data) – Toolbox on essential data protection safeguards for enforcement cooperation between the EEA and third country supervisory authorities – to facilitate the engagement between EDPB members and the SAs of third countries and covering key topics, such as enforceable rights of data subjects, compliance with data protection principles and judicial redress – Joint opinion with EDPS on proposals to extend the Digital COVID Certificate	21 March 2022	Press release Guidelines 02/2022 on the application of Article 60 GDPR Guidelines 3/2022 on Dark patterns in social media platform interfaces Toolbox on essential data protection safeguards for enforcement cooperation between the EEA and third country supervisory authorities Joint opinion with EDPS on proposals to extend the Digital COVID Certificate
Proposed EU Cyber Resilience Act	The EU Commission has issued a call for evidence and public consultation on a proposal for a Regulation on horizontal cybersecurity requirements for digital products and ancillary services (an EU "Cyber Resilience Act"). This Act would complement the NIS Directive and the Cybersecurity Act and would establish streamlined and harmonized requirements for the cybersecurity of digital products (both tangible and intangible) and ancillary services across their whole life cycle. At this stage the Commission is considering alternative policy options: – maintain the status quo	16 March 2022	Consultation details

Development	Summary	Date	Links
	– introduce voluntary measures – ad hoc regulatory intervention – a mixed approach of mandatory and soft rules – a horizontal regulatory intervention (ie the Cyber Resilience Act) The call for evidence and consultation close on 25 May 2022.		
EU and US announce intensified negotiations for new EU-US Privacy Shield framework	In a press statement, the President of the EU Commission, Ursula von der Leyen and US President Joe Biden, announced on 25 March that the EU and the US had found "*an agreement in principle on a new framework for transatlantic data flows*", which will "*enable predictable and trustworthy data flows between the EU and US, safeguarding privacy and civil liberties*". In a separate statement released on the same day, the EU Commissioner for Justice, Didier Reynders, and US Secretary of Commerce, Gina Raimondo confirmed that the US Government and the European Commission had "*decided to intensify negotiations on an enhanced EU-U.S. Privacy Shield framework*", to comply with the *Schrems II* judgment. News of an imminent replacement for the Privacy Shield will be welcomed by organisations that have been scrambling to implement alternative safeguards for transfers of personal data from the EU to the US since the July 2020 judgment in *Schrems II*, which found the EU-US Privacy Shield framework for safeguarding transfers of personal data from the EU to the US to be invalid. However, the development has already attracted criticism from Max Schrems who remarked that "*a political announcement without a solid text, seems to generate even more legal uncertainty for the time being*".	25 March 2022	EU statement US statement Schrems II judgment briefing NOYB statement

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: Use of US web-analytics service by Austrian website violates GDPR	In a landmark decision, the Austrian Data Protection Authority ("**DPA**") ruled that an Austrian website's use of a web analytics tool from a major US-based service provider violates GDPR. The decision was the first ruling in response to the 101 complaints filed by Austrian NGO NOYB, in respect of which the EDPB created a special task force. The website concerned had implemented the cookie-based web-analytics tool on its website. The service provider offering this tool collects data about the use of the website via unique identifiers stored in cookies, as well as other data such as the user's IP address, and processes the data in the United States. A data subject lodged a complaint against the website operator and the service provider. The DPA's decision is not yet legally binding, and the defendant has the right to appeal the decision. In its decision, the DPA ruled that: – Chapter V GDPR is applicable to the transfer of cookie data. The ePrivacy Directive does not contain special rules for data	Date of Decision: Published: 13 January 2022	Official statement by the Austrian DPA (in German) Official anonymized decision text published by the Austrian DPA (in German) Machine Translation of the Decision into English created by noyb

Development	Summary	Date	Links
	transfer and therefore GDPR is applicable and the DPA is also competent – Data subjects have a subjective right to file complaints under Article 77 GDPR based on alleged violations of Chapter V GDPR – Unique identifiers used in cookies are personal data, regardless of whether they can be connected to the user's IP address or name. The possibility to single-out a website user, and to distinguish them from other users based on these identifiers, is sufficient to consider the data connected to it as personal data – 'Singling-out' is to be considered "identification" under GDPR; this is particularly the case when a unique identifier is combined with further data (eg browser data), as the combination of this data renders the "digital footprint" of the user more unique – In any case, analytics data is personal data when the data is or can be connected with a user's account (as was possible for this service provider). This is even the case if the connection is disabled in the user's account, as the identification is technically possible whenever the connection is enabled. This possibility of identification is therefore sufficient to constitute personal data under Article 4(1) GDPR – Regarding the transfer of personal data to the US; the website operator is acting as controller, the analytics service provider is acting as processor; however, the analytics service provider may also be a controller for the further processing of the data, which was not subject to this proceeding – The implementation of the analytics tool by the website operator constitutes a transfer of personal data to a third country, because as a direct consequence of this implementation, data was transmitted to the US – As the analytics service provider is subject to section 702 of the Foreign Intelligence Surveillance Act (FISA) and, as their transparency report specifies, it regularly receives requests from US authorities under this legislation, the DPA		

Development	Summary	Date	Links
	concluded that the EU standard contractual clauses did not provide an appropriate level of data protection. The contractual, organisational and technical supplementary measures taken by the analytics service provider were not to be considered an effective means of ensuring an equivalent level of data protection – Therefore, the website operator violated Article 44 GDPR by allowing this data transfer – However, the DPA found that the analytics service provider as data importer had not violated Article 44 GDPR, because it had not carried out a transfer of personal data As the website operator has since merged with a German company, this case has been referred to the responsible German DPA for further enforcement		
Austrian Ministry of Digital and Economic Affairs announces EUR 2.3 million in subsidies for SMEs investing in cybersecurity	To combat the increasing risk of cybercrime for small and medium-sized enterprises (SMEs), the Austrian Ministry of Digital and Economic Affairs has announced a new cybersecurity subsidy programme for SMEs with a total funding sum of EUR 2.3 million. Starting from 1 April 2022, Austrian SMEs can receive a refund of up to 40% of their investments in the area of cybersecurity (capped at EUR 20,000 per SME).	21 March 2022	Announcement (in German) Subsidy page (in German)
Austrian DPA issues EUR 8 million GDPR fine against supermarket chain	The Austrian DPA has reportedly issued a GDPR fine of EUR 8 million against an Austrian supermarket chain regarding their use of customer data in connection with a customer loyalty program. The decision is not yet legally binding, and the supermarket chain announced that they would appeal against the decision. The decision has been reported on in the media, but the DPA has not published its decision at the time of writing.	14 January 2022	Media coverage (in German)
Austrian Federal Administrative Court: A child's wishes and interests must be taken into account when granting parents access to child's data	The Federal Administrative Court recently made a decision in a case relating to the sharing of a child's personal data by psychiatric clinic with the child's parents. In the case, the parents of a 12 year-old child requested access to the child'scomplete patient file held by the psychiatric clinic.	Date of Decision: 14 January 2022 Published: 2 February 2022	Decision (in German)

Development	Summary	Date	Links
	Within the request, the child's parents relied on the child's right to access under Article 15 GDPR, which they were asserting as the child's representatives. However, the child had previously expressed to the doctors at the psychiatric clinic that it was their wish that their parents should not have access to certain data. The court confirmed in its ruling that the psychiatric clinic had rightfully refused to provide the applicable data to the child's parents. Despite being the child's legal representatives, who can, in principle, exercise a child's data subject rights, it was confirmed in this case that this principle only applies to the extent that to do so does not conflict with the child's interests. It should be noted that children also have certain rights of participation in these decisions, depending on their cognitive maturity. The first level to consider is a child's right to be heard in the decision-making process. If the child reaches the necessary mental cognitive maturity to assess the data processing and its consequences, he or she can participate in the decision making to a greater extent, up to and including a joint or autonomous decision. According to the Court, this cannot always be assessed based on age, so will depend on the maturity of the child in the individual case. In this case, the court concluded that the 12-year-old child had sufficient insight and judgment with regards to the processing and consequences of the applicable disclosure. Therefore, the child had the right to object to the disclosure of certain aspects of their medical record being shared with theirparents. Therefore, the clinic was correct in refusing to share these relevant aspects of the child's information with the parents.		
Austrian DPA publishes quarterly newsletter	The Austrian DPA has published its most recent quarterly newsletter, whichfocuses on its position in relation to the Austrian Parliament's draft Mandatory Vaccination Bill, recent activities by the EDPB and selected decisions in the last quarter.	18 January 2022	Link to newsletter (in German)
Austrian DPA issues critical statement on draft Mandatory Vaccination Bill	The Austrian DPA has issued a critical statement on the Austrian Parliament's draft Mandatory Vaccination Bill.	4 January 2022	Statement (in German)

Development	Summary	Date	Links
	The following points were made from a data protection perspective: – The draft does not mention the specific legal basis under Article 9(2) GDPR being used for the data processing of vaccination data under the bill. It should instead be made clear which of the exemption provisions of Article 9(2) GDPR are being used – The bill should specify which categories of personal data will be processed by the authorities under the bill – The bill (in the opinion of the DPA) allows for the use of more personal data for identification purposes than necessary – The bill allows the Federal Minister for Health to use public entities as processors. However, it is not clear whether the required data processing agreements under Article 28 GDPR have been concluded A data protection impact assessment has not been conducted.		
Austrian DPA: Codes of conduct under GDPR cannot apply to only one controller	The Austrian DPA denied an application for the approval of a code of conduct under Article 40 GDPR. The application for the code of conduct was made by a company acting as controller, and the code was intended to apply only to the applicant itself. The DPA ruled that codes of conduct cannot be applied for by individual companies, but only by associations and representative bodies. Furthermore, codes of conduct have to be relevant to more than one controller. The decision is not yet legally binding.	18 January 2022	Summary of decision in the DPA's newsletter (in German)
Austrian Federal Administrative Court: Data transfer from controller to processor does not require a lawful basis under Article 6 or Article 9 GDPR	The Federal Administrative Court ruled that a controller does not need a separate lawful basis under Article 6 and/or Article 9 GDPR in order to transfer personal data to a processor. As the processor will only process the personal data on the instructions of the controller, the data processing by the controller and processor can be considered as a single processing operation, for which only a single assessment of lawfulness is required.	Date of Decision: 18 January 2022 Published: 18 January 2022	Link to Decision (in German)

Austria

Development	Summary	Date	Links
Austrian Federal Administrative Court confirms strict opt-in requirement for tracking cookies	In a decision regarding the approval of a code of conduct under Article 40 GDPR, the Federal Administrative Court confirmed the requirements of the Article 5(3) ePrivacy-Directive and its Austrian implementation for the use of cookies. In particular, the use of cookies requires the user's prior consent if they are not "strictly necessary" in order for the provision of an information society service explicitly requested by the user to provide the service or for the transfer of a communication. The Court confirmed that the requirement for cookies to be "strictly necessary" should be considered in a technical sense and not in an economical sense. Tracking cookies which a website operator claims to need because the site could not be operated without the revenue from advertising based on these cookies are not to be considered "strictly necessary" and require the user's consent.	Date of Decision: 18 January 2022 Published: 20 January 2022	Decision (in German)
Austrian Administrative Supreme Court: The DPA cannot rule separately on permissibility of processing in *ex officio* proceedings	The Austrian Administrative Supreme Court ruled that in GDPR proceedings initiated *ex officio* by the DPA, the DPA is not entitled to issue a separate ruling on the permissibility of the processing itself, as issuing such a ruling is not listed as a DPA power under Article 58 GDPR. Whilst such a decision on the permissibility of a processing operation will be an implicit requirement for the exercise of the DPA's powers under Article 58 GDPR, there is no legal basis for the DPA to issue a separate decision on the permissibility of processing. Such a decision is only possible in proceedings initiated by a data subject complaint.	Date of Decision: 18 January 2022 Published: 20 January 2022	Decision (in German)
Austrian Administrative Supreme Court: Marketing data on assumed political affinity is special category personal data under Article 9 GDPR	The Austrian Administrative Supreme Court has ruled on an appeal by a large postal services provider in Austria, following a complaint made by a data subject. The defendant had used public and non-public data (such as age, home address, education and published results of political elections) to assign certain assumed characteristics to people living in Austria, including their assumed political affinity. This data was then sold for marketing purposes, without the data subjects' consent.	Date of Decision: 18 January 2022 Published: 21 January 2022	Decision (in German)

Development	Summary	Date	Links
	The Administrative Supreme Court confirmed the underlying ruling by the DPA, ordering the controller to cease the processing of such data, and delete all data regarding assumed political affinity. It ruled that such assumptions or predictions of political affinity constitute special categories of personal data under Article 9 GDPR. As the defendant could not base itsprocessing on one of the exemptions of Article 9(2) GDPR, the processing was deemed to be unlawful.		
Austrian Administrative Supreme Court suspends proceeding on GDPR fine of EUR 18 million in anticipation of CJEU ruling	The Austrian DPA issued a fine of EUR 18 million against a large postal services provider in Austria, following a complaint made by a data subject in relation to the company's processing of data relating to assumed political affiliation (see update above). The Federal Administrative Court overturned this decision and repealed the fine on the basis that the DPA had failed to demonstrate that the GDPR contravention by the postal services provider was caused by the culpable behavior of its representatives or employees. The DPA appealed against this decision to the Austrian Administrative Supreme Court. The Administrative Supreme Court has suspended the proceeding in anticipation of the Court of Justice of the European Union's ("**CJEU**") preliminary ruling in *Case C-807/21*. In this case, a German court has asked the CJEU to clarify whether Article 83 GDPR is to be interpreted as to allow GDPR fines to be issued directly to a legal person, without requiring a finding that an identified natural person committed a violation of GDPR.	Date of Decision: 18 January 2022 Published: 28 March 2022	Decision (in German)
Austrian Administrative Supreme Court refers question to the CJEU on applicability of GDPR on Parliamentary Investigating Committees	The Austrian Administrative Supreme Court has requested a preliminary ruling from the CJEU on whether EU law (and therefore the GDPR) is applicable to investigations conducted by a parliamentary investigating committee (Parlamentarischer Untersuchungsausschuss). The court has also asked whether the Austrian DPA would be competent for investigating violations of GDPR by such a committee.	Date of Decision: 18 January 2022 Published: 27 January 2022	Decision (in German)

Development	Summary	Date	Links
	This request followed a complaint by a data subject who had been interrogated by a Parliamentary Investigation Committee, and the minutes of the interrogation were subsequentlypublished on the Parliament's website without being anonymised. The complainant therefore considered this a violation of GDPR.		
Austrian Data Protection Authority rules that a map of Islamic organizations does not violate GDPR	An Austrian university had compiled a list of all active Islamic organisations in Austria, eg all organisations operating a mosque. These organisations were marked on an interactive map, which was then published for use as an online tool. A Muslim youth organisation and several natural persons filed a complaint against the tool, on the ground that the tool infringed their right to data protection (which applies to legal persons to a certain degree in Austria), as it had attracted attention from right-wing political activists. The complainants also argued that some of their private addresses were disclosed to the public. The Austrian Data Protection Authority decided that the tool did not infringe the complainants' right to data protection, as it could neither be determined from the tool, nor from the public register, whether any of the addresses in the tool were those of private individuals. It did seem that several officials of such organisations may have registered their associations on the public register by using their private addresses, but this could not be determined and the DPA did not consider this data to be the personal data of the officials. The DPA further stated that the tool provided an important contribution to academic and media research on the topic of political Islam in Austria, andtherefore the interests of academic freedom and freedom of expression provided by the tool overweighed the interests of the organisations included. The decision has been made public via several media reports, but the DPA has not published the decision. Some of the complainants have stated that they intend to file an appeal.	9 February 2022	Media report (in German)
Austrian Supreme Court rules that teacher evaluation app was not in	A pupil programmed and provided a teacher evaluation app, which enabled pupils to provide 1-5 star reviews of teachers in	Date of Decision: 9 February 2022	Decision (in German)

Development	Summary	Date	Links
violation of GDPR (Update to Updata Edition 14)	specific categories, but did not provide for the publication of comments. The app was aimed at pupils to review their teachers, and restricted users to reviewing staff at a single school. The teachers' overall mean scores were available under their names, but could only be accessed by first accessing the specific school. App users' identities were not verified, but the verification of cell phone numbers applied in order to reduce the risk of one user creating multiple accounts. The Austrian DPA commenced an *ex officio* review, but closed the proceeding, finding that there had been no GDPR violation. As reported in Updata Edition 14, the Austrian Administrative Supreme Court upheld this finding against several appeals from teachers. One teacher filed a civil action to have the provider cease subjecting them to anonymous reviews, in addition to disclosing their name, teaching subject and place of work. They claimed an illegitimate infringement of their rights to data protection under GDPR, and privacy under ECHR and CFR, based on incorrect reviews and the risk of misuse by users that were not actually pupils. Furthermore, it was asserted that no remedies were provided against these risks, and neither the provider, nor the pupils or public had an interest in reviewing individual teachers. Instead it was claimed that due to parents' and pupils' choices being limited to schools, the only legitimate interest in this case may be a general review of schools. The Higher Regional Court, as the court of second instance, partially ruled in favour of the claimant (as reported in Updata Edition 14), against which the respondent appealed. The Supreme Court subsequently issued its final decision. The respondent was not successful in claiming media privilege, as the Supreme Court did not identify any journalistic quality to simply displaying the mean value of 1-5 stars reviews. Additionally, the argument of the closure of the DPA's *ex officio* review constituting a legal precedent for the civil courts was also unsuccessful.	Published: 21 February 2022	

Development	Summary	Date	Links
	The Supreme Court also asserted that anonymous reviews of identified teachers were covered by the fundamental freedom of expression. Only allowing identified reviews would deter the expression of opinions and would hinder the exercise of fundamental freedoms. The Supreme Court noted that in this case the claimant's privacy was not infringed upon because, due to the reviews only covering professional or social life, it was outweighed by the interest of freedom of expression. The claim against the app provider was dismissed.		
Austrian DPA: Law firm filing evidence to a court without disclosing its source does not violate GDPR	A law firm representing the former employer of the complainant in a labor court proceeding, filed a medical report about the drug use of the complainant as evidence to substantiateits client's case. The complainant filed a data access request to the law firm and requested it be informed about the source of the provision of the medical form. The law firm refused to disclose the source, relying on attorney-client privilege. The complainant therefore filed a complaint against the law firm at the Austrian DPA. The DPA ruled that the law firm was entitled to refuse disclosure of the source, based on attorney-client-privilege. The DPA further ruled that the filing of the report to the court was lawful based on Article 9 (1)(f) GDPR. The complaint was therefore dismissed.	Date of Decision: 9 February 2022 Published: 3 March 2022	Decision (in German)
Austrian Federal Administrative Court: Controllers may respond to data access requests under Article 15 GDPR referring to large amounts of data in a two-step-process	The Federal Administrative Court ruled on an appeal against a DPA decision relating to a complaint regarding an alleged incomplete response to a data access request under Article 15 GDPR. In this decision, the court ruled that in the case of a very general data access request referring to a large amount of processed data, it is permissible for the controller to initially provide the master data as part of a two-stage information procedure. The provision of more comprehensive information can then be provided upon the explicit request by the data subject. However,	Date of Decision: 9 February 2022 Published: 18 January 2022	Decision (in German)

Development	Summary	Date	Links
	this is only permissible if the data subject is explicitly informed of this approach.		

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
Belgian DPA reconfirms cookie consent rules in cookie enforcement case	The Litigation Chamber of the Belgian Data Protection Authority ("**DPA**") issued a decision on 21 January 2022 on a cross border complaint relating to cookies. The decision sets out the conditions under which companies are allowed to track online user behaviour, and whether consent must always be obtained. The decision is valuable as the Litigation Chamber provided some background on the subject of cookies, and recalled the basic legal principles concerning tools for tracking internet users. The Litigation Chamber of the DPA ruled the following: – A breach of Articles 12 and 13 GDPR – when users logged onto the defendant's website (homepage), a first-party cookie, which could be described as 'essential', was already loaded in the browser, although no prior information was provided to the user. The obligation to provide prior information applies to all types of cookies, regardless of whether or not their impact on the data subject's right to data protection is low. – It is not enough to comply with the transparency obligation of Article 13 GDPR if the screen before entering the website	21 January 2022	Decision (French) Decision (English)

Development	Summary	Date	Links
	(when selecting the language and country choice) states: "*This website collects and uses non-identifiable information to analyse site activity to improve navigation. You can control how this information is collected and used*" and is accompanied by a hyperlink to a "Privacy policy" page. Before consent is requested, precise information, in clear and simple terms that are easily understandable by the majority of the intended website visitors, must be displayed and cover: – the identity of the controller – the purpose of the cookies/other trackers that will be installed and/or read – the data they collect – their lifetime – the data subject's rights (including the right to lodge a complaint and the right to withdraw consent) It was therefore considered irrelevant what impact the type of cookie has on the data subject. Furthermore, it was asserted that a hyperlink in a banner should lead a data subject to the information required about cookies, instead of to the general privacy policy. It should also be noted that it was asserted in this case thateven if a website is aimed at French and/or Dutch-speaking audiences, it is considered appropriate to display the warning regarding the use of cookies in English, as it is a widespread language commonly used by other websites before selecting a user's language. – The "cookie wall" practice (ie where a user is obliged to accept cookies in order to use a website in a normal way) is only permitted when the rejected cookie is strictly necessary (as opposed to a non-functional cookie). For non-functional cookies, the user must be able to accept or refuse the setting, without coercion, which means that the user cannot be refused certain services or benefits when consent is not given. The record of processing activities must also indicate and easily identify the third countries to which personal data is sent. This is		

Development	Summary	Date	Links
	particularly important and applicable in light of the *Schrems II* judgment.		
Ruling regarding the mass processing of social media data regarding political story	On 27 January 2022, the Belgian DPA imposed a fine of EUR 2,700 on a Belgian NGO and of EUR 1,200 on one of its volunteer researchers (the "defendants") for breach of the GDPR rules. This was in the context of a study on the possible political origin of posts on Twitter concerning the "Benalla affair", an incident relating to the French President's security officer. Even before the publication of the result, the defendants published the analysed raw data, including the personal data of a large number of people. The Belgian DPA and the Commission Nationale d'Information et Libertés ("**CNIL**") received more than 200 complaints about the use of personal data from 55,000 Twitter accounts. The Belgian DPA ruled the following: – In this case, the exemption for scientific research could not be relied upon, since it requires additional safeguards under Article 89 GDPR (i.e pseudonymisation - which was not carried out properly here). In addition, the exemption for journalistic purposes could also not be relied upon, since this exemption had not yet been implemented into Belgian law at the time the events took place – Even if personal data is published on social media, the GDPR – and therefore the purpose limitation principle – still applies. The DPA held that a legitimate interest could only be relied upon if: (i) the processing was limited to what was strictly necessary for the purpose; and (ii) the legitimate interest is balanced against the rights and freedoms of the data subjects In short, the DPA stated that the study lacked a legal basis due to the disproportionate infringement of the rights of the authors of the posts (tweets) concerned. There were also insufficient safeguards – eg no pseudonymisation – and the data subjects risked potential reputational harm and discrimination; Furthermore, the defendants did not have a clear data protection notice, a record of processing activities and/or contracts with	27 January 2022	Decision (Dutch)

Development	Summary	Date	Links
	processors. They also did not carry out a data protection impact assessment (a "DPIA"), even though the study concerned sensitive categories of data (eg political affinities).		
Belgian DPA decides that IAB Europe's Transparency and Consent Framework violates key provisions of the GDPR	We mentioned in our previous Updata contribution that the DPA was expecting to issue an important decision regarding the IAB Europe's Transparency and Consent Framework (the "**TCF**"). As a reminder, the IAB Europe's TCF is the global cross-industry effort to help publishers, technology vendors, agencies and advertisers meet the transparency and user choice requirements (ie collecting consent to cookies) under the GDPR. The DPA issued the expected decision on 2 February 2022, and identified that the TFC infringes key provisions of the GDPR. The key findings were: – IAB Europe is considered to be a controller of the personal data collected and distributed through the TCF, even though it does not itself collect and store the personal data – It enables the generation of the transparency and consent string (the "**TC string**") and sets the policies for how consents could be obtained and disseminated, which is a form of exerting control over the purposes and essential means of the processing. IAB Europe did not comply with a number of controller obligations, including keeping a record of processing activities, the appointing of a DPO and the carrying out of a DPIA – There is a joint controllership between IAB Europe and other adtech players (publishers, participating adtech vendors and consent management platforms ("CMPs")) for the collection and dissemination of user preferences, objections and consents and the subsequent processing of their personal data – There is no legal basis for the processing of user preferences in the form of a TC string. The DPA stated that (i) the consent (obtained through CMPs) is insufficiently free, specific, informed and unambiguous and (ii) the legitimate interest is prohibited as a legal basis for participating in TCF in its current format	2 February 2022	Decision (English) Decision (Dutch)Link

Development	Summary	Date	Links
	– The information provided via the CMP interface is too general and vague for users to understand the nature and scope of the processing, in particular given the complexity of the TCF – so the transparency requirements of the GDPR are not met – Organizational and technical measures in accordance with the principle of data protection by design and by default were not taken in order to ensure the effective exercise of the rights of data subjects and to check the validity and integrity of user choices (among other things) The DPA imposed a fine of EUR 250,000 on IAB Europe and imposed a deadline of two months to reform its practices and introduce an action plan where it shows how it will bring the TCF framework into compliance. The IAB must also permanently delete any personal data which was already processed under the TCF from its systems. IAB Europe has appealed this decision to the Market Court. This decision has a significant impact on the adtech sector where a lot of publishers and adtech vendors rely on the TCF to demonstrate their own compliance to the GDPR.		
Interplay between request for access to audio recording and maximum retention period	The Belgian DPA received a complaint following a request for access to an audio recording of a telephone conversation with the Flemish Tax Administration. However, the Flemish Tax Administration could not grant access to the file as it had already deleted the recording in line with its one-month retention period. The Litigation Chamber of the DPA acknowledged the data subject's right to lodge a complaint with the DPA. However, it decided to dismiss the complaint because the Flemish Tax Administration has a certain degree of discretion regarding the retention period of telephone conversation recordings, which may not in any event exceed a maximum retention period of one month. It should be noted that the complainant also acknowledged that he was informed about this limited storage period.	11 February 2022	Decision (Dutch)

Development	Summary	Date	Links
Belgian DPA issues decision concerning search engine operator's de-listing refusal	On 17 March 2022, the Belgian DPA issued a decision concerning a search engine operator's refusal to 'de-list' disputed links, and therefore, to not grant a complainant's request for deletion. The case also concerned the issue of determining which corporate entity was liable for compliance. Regarding the liability issue, the DPA gave the following reasoning: – The first defendant had nothing to do with the processing activities and should therefore not be part of the proceedings – The second defendant was considered to be the controller for the processing activities at stake. It had invoked Article 3(1) GDPR, instead of Article 3(2) GDPR, which resulted in the third defendant being its EU representative – The processing activities at stake could be attributed to the third defendant because its activities were inextricably linked to those of the controller. This implied that the DPA could impose liability on the third defendant, even though it was not considered a controller for the processing activities The impact of this is that when (i) international undertakings have EU establishments and (ii) the processing activities of the non-EU controller is inextricably linked to the EU establishment, the latter could be responsible for non-compliance with GDPR obligations. As for the substantive issue, ie the refusal to de-list, this complaint was rejected by the Belgian DPA. The search engine operator had stated there was a public interest in maintaining access to the press articles covered by the complaint. The Belgian DPA took into account the severity of the facts (i.e the relevant criminal offences and offences to the professional code of conduct), their relatively recent nature (i.e the timeframe of the actions), their relevance to the complainant's current professional activity and the quality of the latter – both today and even more so at the time of the facts. The Belgian DPA decided to classify the complaint without follow-up against the defendants.	17 March 2022	Decision (French)

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
Administrative Provisions on Mobile Internet Applications Information Services (Draft for Comment) **《移动互联网应用程序信息服务管理规定（征求意见稿）》**	On 5 January 2022, the Cyberspace Administration of China issued the Administrative Provisions on Mobile Internet Applications Information Services (Draft for Comment) for public consultation by 20 January 2022. The Draft for Comment underlines China's commitment to regulating the privacy and security position for mobile internet application information services. We have set out below the key points of the Draft for Comment in relation to the requirements for application providers: – Authentication of users' identity: Where the application provides users with services such as information publication and instant messaging, the identity of the users applying for registration shall be authenticated. Where users do not provide proof of identity or fraudulently use another person's identity for false registration, they must not be provided with the relevant services – Full-process data security management system: Application providers shall deploy technical measures (such as warnings, limiting functions and closing accounts to address violations) to ensure data security and establish full-process mechanisms of data security management	5 January 2022	Link to Draft (Chinese)

Development	Summary	Date	Links
	– Necessary scope of consent: Users shall not be compelled to consent to unnecessary handling of personal data for any reason, and users must not be denied access to the basic functions and services of an application because they did not give consent to such non-essential processing Protection of minors: Application providers shall strictly comply with the requirements for registration in the users actual name and login requirements for minors' accounts. They must not provide minor users with products and services which induce any form of internet addiction.		
Information Security Technology - Guideline for Identification of Critical Data (Draft for Comment) **《信息安全技术** **重要数据识别指南（征求意见稿）》**	On 13 January 2022, the National Information Security Standardization Technical Committee published the Information Security Technology – Guideline for Identification of Critical Data (Draft for Comment) ("**Draft for Comment**") for public consultation by 13 March 2022. The publication aligned with the full enforcement of the Data Security Law which came into force on 1 September 2021. The Draft for Comment sets out six underlying principles for identifying critical data: – Focus on security impacts: Data shall be assessed based on its security impact from the perspective of national security, economic operation, social stability, public health and safety and other factors – Highlight of area(s) of focus for protection: Data shall be classified and key points for security protection shall be specified and critical data shall be subject to additional security protection requirements to ensure the free flow of non-critical data – Bridging with existing regulations: The existing local regulations and industry practices shall be fully considered. – Comprehensive risk assessment: Risks shall be assessed in a holistic matter covering an array of factors, including confidentiality, completeness, availability, authenticity and accuracy of data and other factors	13 January 2022	Link to Guidance (Chinese)

Development	Summary	Date	Links
	– Qualitative and quantitative approaches: Both qualitative and quantitative methods shall be adopted in identifying critical data – Active assessment: The critical data shall be reassessed according to the change in purpose of use, method of sharing and importance and other factors The Draft for Comment further outlines 14 factors as pointers for identifying critical data.		
Information Security Technology - Basic Requirements for Competence for Cyber Security Workforce (Draft for Comment) **《信息安全技术** **网络安全从业人员能力基本要求（征求意见稿）》**	On 17 January 2022, National Information Security Standardization Technical Committee published the Information Security Technology - Basic Requirements for Competence for Cyber Security Workforce (Draft for Comment) for public consultation by 18 March 2022. The Draft for Comment is applicable for the selection, training, assessment and management of cyber security practitioners by various organisations such as government bodies, network operators, network security education providers and scientific research institutions. The Draft for Comment sets out general knowledge and technical requirements, and further classifies the workforce into five categories (cyber security managers, cyber security constructors, cyber security operators, cyber security auditors and evaluators and cyber security research and education personnel) and outlines the corresponding knowledge and skillset different types of practitioners shall possess.	17 January 2022	Draft Guidance (Chinese)
Administrative Measures for Deep Synthesis of Internet Information Services (Draft for Comment) **《互联网信息服务深度合成管理规定（征求意见稿）》**	On 28 January 2022, the Cyberspace Administration of China ("**CAC**") published the Administrative Measures for Deep Synthesis of Internet Information Services (Draft for Comment) for public consultation by 28 February 2022. The Draft for Comment consists of 25 articles, which primarily outline the requirements for the following five categories: – Purpose, scope and general requirements: The purpose for the formulation of this rule, scope of application and general requirements	28 January 2022	Draft Measures (Chinese)

Development	Summary	Date	Links
	– Main responsibilities of deep synthesis service providers: This is required to establish and improve management systems for areas including algorithm mechanism review, information content management and employee training and having safe and controllable technical security measures in place for the development of new technologies and applications – Management system for identification of deep synthesis information: The deep synthesis service providers are required to insert a logo and store log information in accordance with the law so that deep synthesis information could be identified and traced by itself – Supervision and management: Internet application store service providers shall be responsible for managing the security of deep synthesis applications, verifying the security assessment and filing of the same, and implementing timely measures where state requirements are violated Legal responsibility, governing bodyand implementation date: Violations of the Draft Measures shall be handled by the cyberspace administrations of the state, provinces, autonomous regions and municipalities. The provisions therein shall be interpreted by the CAC.		
Information Security Technology - Guideline for Life Cycle Security Management of Mobile Internet Apps (Draft for Comment) **《信息安全技术** **移动互联网应用程序（App）生命周期安全** **管理指南（征求意见稿）》**	On 8 February 2022, the National Information Security Standardisation Technical Committee published the Information Security Technology - Guideline for Life Cycle Security Management of Mobile Internet Apps (Draft for Comment) for public consultation by 9 April 2022. In particular, the Draft for Comment provides guidelines on the security management of mobile applications which are applicable to the development and operation of applications by developers, mobile application distribution platform manufacturers and mobile smart terminal manufacturers ("**Relevant Parties**"). The Draft for Comment divides the life cycle of apps into seven stages: requirements analysis, development design, test verification, launch, installation and operation, update and maintenance, and termination. Various security risks may arise during the entire lifecycle, requiring security analysis and security management to be implemented for each stage. Security	8 February 2022	Draft Guidance (Chinese)

Development	Summary	Date	Links
	recommendations both during application development and throughout the lifecycle have been highlighted, which include amongst others: – Access control: The Draft for Comment recommends unique authentication for individual users and assignment of their corresponding access rights. The complexity of passwords could be adjusted based on the practical needs of the user and in conformity with security policies; it is good practice for passwords not to be displayed, stored and transmitted in clear text. The Relevant Parties could actively apply for the authority that their businesses require, but not for access for those aspects unrelated to their business functions. Various measures for log recording and protection could be undertaken as well – Communication security: The Relevant Parties could set unique, random and non-recognisable session identifiers for communication. When conducting important business operations (eg mobile payment and identity authentication), random tokens or parameters could be used – Data protection: Applications could adopt password technology to safeguard the authenticity, completeness and security of data Further, it is recommended that the Relevant Parties work hand-in-hand to facilitate various aspects of life cycle security management.		
Circular on Further Regulating Pre-installation of Apps on Mobile Smart Terminals (Draft for Comment) **《关于进一步规范移动智能终端应用软件预置行为的通告（征求意见稿）》**	On 16 February 2022, the Ministry of Industry and Information Technology issued the Circular on Further Regulating Pre-installation of Apps on Mobile Smart Terminals (Draft for Comment) for public consultation by 3 March 2022. The Draft for Comment aims to standardise the pre-installation of applications on mobile smart terminals, enhance the supply of mobile internet application services, build a safer and more dynamic industrial environment and promote the prosperous development of mobile internet access. The following points are outlined in particular:	16 February 2022	Draft Publication (Chinese)

Development	Summary	Date	Links
	– Underlying principles: The pre-installation of applications on mobile smart terminals shall abide by the principles of: compliance, "user first", safety and convenience and minimum necessity amongst other principles – Option to uninstall: Manufacturers shall ensure that, save for basic functional software (eg system setting, file management, multimedia recording, basic communication applications and the application store), all applications pre-installed on mobile smart terminals could be uninstalled. On this basis, safe and convenient uninstallation methods shall be offered to users – Management and control: Manufacturers shall enhance the authority management mechanism for mobile smart terminals, improve the security of operating systems and adopt technical measures to prevent the replacement of operating systems or the installation of application software in the process of product circulation		
Announcement on the Launch of the Internet Information Services Algorithm Filing System **关于互联网信息服务算法备案系统上线的通告**	On 28 February 2022, the Cyberspace Administration of China announced the launch of the Internet Information Services Algorithm Filing System, with effect from 1 March 2022. The announcement highlights that the launch aligns with the requirements of Article 24 of the Internet Information Service Algorithm Recommendation Management Regulations ("**Regulations**") (effective from 1 March 2022), which sets out that algorithm recommendation service providers with public opinion attributes or social mobilisation capabilities shall fill in the name, service, field, algorithm type andalgorithm self-appraisal (and other information) of the service provider through the filing system within ten working days of provision of such service. The announcement further highlights that Article 24 of the Regulations states that, in the event the filing information of algorithm recommendation service provider changes, the change procedures must be carried out within ten working days of the date of change. Similarly, if the algorithm recommends that service providers terminate services, they must complete filing and cancellation procedures within 20 working days from such termination recommendation.	1 March 2022	Announcement (Chinese)

Development	Summary	Date	Links
Administrative Measures for Internet Pop-up Push Services (Draft for Comment) **《互联网弹窗信息推送服务管理规定（征求意见稿）》**	On 2 March 2022, the Cyberspace Administration of China published the Administrative Measures for Internet Pop-up Push Services (Draft for Comment) for public consultation by 17 March 2022. The Draft for Comment specifies the regulations and requirements for internet pop-up push services, including but not limited to the following: – Use of algorithm models: Internet pop-up push services shall not establish algorithm models which (i) violate laws and regulations, or violate ethics and morality in promoting user's addiction and excessive use of services; (ii) abuse personalised pop-up windows or use algorithms to block or excessively recommend any information; (iii) abuse algorithms to create accounts for minor users or push any information to minor users which could possibly affect their physical and mental health – Specific requirements for pop-up windows: It is emphasised that, in using pop-up windows to push any advertisement information, (i) the content compliance review must be passed to not violate relevant national laws and regulations; (ii) such pop-up windows shall be identifiable with the text "advertisement" being noticeably marked and explicitly shown to users; (iii) efforts shall be made to ensure that any pop-up advertisement could be closed with a single click; (iv) user's interests and rights (as well as their experience) shall be protected, there shall be no preferential treatment between ordinary users and VIP users and the user's right to close the pop-up windows shall not be interfered or impacted Not to present information that maliciously attracts and redirects traffic: It is prohibited to (i) present any third-party link, QR code and other information which maliciously attracts traffic and causes a site redirect by means of pop-up information push; or (ii) use pop-up information to coerce user "click throughs" to falsify viewership data and commit traffic hijacking.	2 March 2022	Draft Publication (Chinese)

Development	Summary	Date	Links
Guideline on Corporate Data Compliance - Yangpu District of Shanghai **《企业数据合规指引》-上海市杨浦区**	The People's Procuratorate of Shanghai Yangpu District published the first Guideline on Corporate Data Compliance - Yangpu District of Shanghai. The guidelines are divided into six chapters, helping businesses strengthen data compliance management on the following fronts: – Data compliance management system: The top management level of a business shall be responsible for data compliance and ensuring that the implementation and effectiveness of data compliance measures is included in the business' internal personnel performance appraisal system. Compliance departments shall be set up directly by the board of directors and duties should not be performed by legal departments – Data risk identification: Businesses shall accurately identify risks encountered in compliance management. The Guideline lists out certain prohibited data activities, such as activities which affect or may affect national security, infringe other's legal interests and illegal sales and provisions of data amongst other activities. In particular, processors who process personal information shall comply with the provisions of the Personal Information Protection Law, and delete or anonymise the personal information based on the circumstances – Data risk assessment and disposal: Businessesshall conduct data risk assessments based on their individual operational scales, structures, businesses and the market environment. Comprehensive risk management mechanisms shall be set up to stop activities identified as risky where necessary and promptly implement remedial measures Data compliance operation and security: It is notedthat certain mechanisms (eg compliance consultations, inspection systems, whistleblowing systems and incentive and disciplinary schemes) could be introduced. Businesses could also increase resources for internal data compliance training with management and employees.	26 January 2022	Guidance (Chinese)

Development	Summary	Date	Links
Administration Measures on Public Data of Jiangsu Province **江苏省公共数据管理办法**	On 9 January 2022, the Jiangsu government promulgated the Administration Measures on Public Data of Jiangsu Province (effective from 1 February 2022), which stipulate the establishment of a data protection system in safeguarding confidentiality and personal information of the public. The Measures are categorised into nine chapters and 64 articles, which outline requirements in the following areas: – Supply of public data: Public management service agencies shall be responsible for providing public data which meets quality requirements and shall have the right to apply for the use of public data. The collection of public data shall be in accordance with all laws and regulations and the collection of public data related to personal information shall be restricted to the minimum data necessary for the intended use – Sharing of public data: Public data could be divided into three types based on their "sharingtype": (i) unconditional sharing, (ii) conditional sharing, and (iii) non-sharing. The sharing type of public data between public management and service agencies shall be gratuitous sharing by default, with non-sharing as an exception only – Public access of public data: Public data could be divided into three types based on their ease of access: (i) not open, (ii) conditionally open and(iii) unconditionally open. The access of public data shall depend on the needs of businesses and the public and such access shall be in a legal, safe and orderly manner – Utilisation of public data: Local people's governments above the county level shall use public data to develop and improve the data factor market, and support and promote the use of public data in various sectors Safety management: The Measures specify requirements for coordinating digital development and security, establishing and improving data security governance systems, strengthening the whole-process protection of public data security and improving data security capabilities.	1 February 2022	Publication (Chinese)

Development	Summary	Date	Links
Guangdong Province Public Data Security Management Measures (Draft for Comment) **《广东省公共数据安全管理办法（征求意见稿）》**	On 7 February 2022, the Government Service Data Administration of the Guangdong Province published the Guangdong Province Public Data Security Management Measures (Draft for Comment) for public consultation by 21 February 2022. The Draft for Comment consists of six chapters and 32 articles, which outline the requirements for the following: – Fundamental institutional systems: Mechanisms for registration filing, grading and classification of public data, security systems by grading and commercial cryptographic application, correction of public data and deletion of public data shall be in place – Full-lifecycle data security management: The Draft Measures set out the requirements for ensuring security of data collection, data storage, use and processing of data, data transfer, data provision and public access of data – Data security support system: There shall be a centralised uniform mechanism in place for risk assessment, reporting, information sharing, monitoring and early warnings. Further, specific emphasis shall be placed on risk supervision and assessment, emergency response, security audit, security management by delegated parties and personnel management Supervision and legal responsibility: Public data authorities at all levels shall establish and improve data security monitoring, early warnings and information report systems. The Draft Measures also set out the responsibilities of public data authorities, other authorities and public administration and service agencies.	7 February 2022	Publication (Chinese)
Regulation of Zhejiang Province on Public Data **浙江省公共数据条例**	The Regulation of Zhejiang Province on Public Data came into effect on 1 March 2022. Consisting of eight chapters and 51 articles, the Regulation outlines the scope of public data, platform construction specifications, collection and aggregation rules, sharing and opening mechanisms, authorised operation systems and security management specifications.	1 March 2022	Regulation (Chinese)

Development	Summary	Date	Links
	The Regulation includes a specific chapter on public data security, with has set out systematic and substantive institutional designs for strengthening public data security management and standardising public data security behaviors: – Institutional system: Institutional systems, such as systems for public data classification, security review, risk assessment, detection and early warning, emergency drills, security audits and destruction shall be set up and improved – Technical protection system: The technical standards and specifications for public data security shall be established and improved in accordance with the requirements of classified and graded protection levels. Technical measures, such as identity authentication, access control, data encryption, data desensitisation, data traceability, data back-up and privacy computing shall be undertaken to improve data security capabilities Operational management system: A normalised operational management mechanism for data security has to be established. The security management of data activities carried out by way of service outsourcing has to be strengthened, which shall effectively prevent the illegal acquisition, tampering, leakage or improper use of public data and protection of personal information, trade secrets and confidential business information and other activities.		

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
Cookies legislation update – Amendment to the Electronic Communications Act	On 1 January 2022, an amendment to the Czech Electronic Communications Act came into force. The legislation brings a major change to the use of website cookies, allowing only the so-called "opt-in" regime. This effectively means that before the website user freely gives their consent, websites cannot collect any user data save for that which is strictly necessary for website functioning. Before this change, websites could collect the data without prior consent, subject to a respective notification, and only needed to cease doing so when the user specifically opted out (the so-called "opt-out" regime).	1 January 2022	ES briefing (Czech)
Office for Personal Data Protection releases the 2022 Inspection plan	The Czech Office for Personal Data Protection has released an inspection plan for 2022. In the plan, the Office aims to carry out inspections of: – compliance with new legal requirements for the use of website cookies and the collection of consents and related data processing; – distribution of commercial communications in compliance with legal requirements; and – controllers from the private and public sector regarding their processing and collection of personal data in certain specified fields such as the use of audio recordings or the use of processors by Czech municipalities.	31 January 2022	Press release (Czech)

Czech Republic

Development	Summary	Date	Links
Whistleblowing legislation process restarted	In accordance with the EU Whistleblowing Directive, the Czech Republic needs to pass implementing national legislation which will protect individuals reporting breaches of law. The Czech Republic failed to finish the legislative process to transpose the directive before the December 2021 deadline and a new government has been formed since. Therefore, the process came to a halt. According to the information available, the process has been restarted and the Ministries are now working on the draft once again, aiming to present the legislation to the government in May / September 2022.	March 2022	Whistleblowing Directive tracker

France

Contributors

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

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

Charlotte Haddad
Associate
charlottehaddad@
eversheds-sutherland.com

Edouard Burlet
Associate
edouardburlet@
eversheds-sutherland.com

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

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

Camille Larreur
Associate
camillelarreur@
eversheds-sutherland.com

Clémence Dubois Ahlqvist
Associate
clemenceduboisahlqvist@
eversheds-sutherland.com

Killian Lefevre
Associate
killianlefevre@
eversheds-sutherland.com

Naomi Bellaiche
Associate
naomibellaiche@
eversheds-sutherland.com

Development	Summary	Date	Links
French mobile telephone operator fined EUR 300,000 for failing to comply with data subjects' requests and protect the security of personal data	The Commision Nationale Informatique & Libertés ("**CNIL**") received several complaints from data subjects having difficulties obtaining responses from one of the main French mobile telephone operators, in particular regarding their access requests and their requests to opt-out from marketing messages. The CNIL therefore invesitgated the matters and it was revealed	CNIL's statement (in French): 1 March 2022 CNIL's deliberation (in French): 28 December 2021	CNIL statement (in French) CNIL deliberation (in French)

Development	Summary	Date	Links
	that the company had not complied with its obligations regarding data subjects' rights, with the requirement to ensure "privacy by design", and with its obligations relating to personal data security. More specifically, the CNIL ruled that the company committed four breaches under GDPR: – non-compliance with Article 15 GDPR (relating to the right of access of data subjects), as the company did not respond to the access requests made by the complainants within the applicable timeline; – non-compliance with Article 21 GDPR (relating to the right to object, including to direct marketing), as the company did address the requests of the complainants who asked to no longer send them marketing messages; – a breach of the obligation to ensure "data protection by design" (Article 25 GDPR), as the company kept sending invoices to complainants whose telephone subscriptions had been cancelled; – a breach of the obligation to protect the security of personal data (Article 32 GDPR), as the company communicated users' passwords via email, in clear text, and the passwords were not temporary (ie.e. did not requre users to change them). As a result, the restricted committee of the CNIL imposed a EUR 300,000 fine on the mobile operator. The CNIL also decided to make the sanction public, to stress the importance of responding to requests relating to data subjects' rights and of ensuring the security of personal data.		
CNIL statement on employees' right of access to their work-related data and e-mails	The CNIL recently released a statement about access requests sent by employees to their employers. The guidance reminds employers that the purpose of the right of access is to allow an individuals to know whether their data is being processed and for which purposes, and to obtain communication of their personal data in an understandable format. In particular, this enables data subjects to verify the	5 January 2022	CNIL statement (in French)

Development	Summary	Date	Links
	accuracy of their data and, if necessary, to rectify or delete it. The CNIL specifies that, specifically regarding access requests from employees: – The employer must have certainty about the identity of the person making the request: if it has reasonable doubts, it may ask for additional information to confirm the identity of the requestor (provided that such information is relevant and proportionate) – The employer shall respond to the request for free. However, in some specific situations, such as where additional copies of the data are requested, a reasonable fee for processing the request may be charged to the employee – The right of access relates only to personal data, not to documents – an employee may not request specific documents through an access request, however the employer may communicate to the employee documents rather than only data if this is more convenient – The exercise of the right of access must not infringe the rights of third parties (eg trade secrets, intellectual property, right to privacy, secrecy of correspondence, etc.). The employer must only provide access to data if doing so does not disproportionately infringe the rights of others but it cannot completely refuse to comply with the request The CNIL also explain how to respond to an employee who wishes to access or obtain copies of work-related emails. In particular, the employer must assess whether such communication would infringe on the rights of third parties, and must therefore distinguish between the messages that can be communicated and those that cannot. This will depend on whether the requesting employee is: 1. the sender or the recipient of the e-mails: where the employee has already had knowledge of the information contained in the emails mentioned in the request, there is a presumption that the disclosure of such e-mails does not infringe on the rights of third parties. However, in specific cases, the employer may argue that access to or disclosure		

Development	Summary	Date	Links
	of e-mails which were already seen by the requestor may still create a risk for third parties (eg if the email contains information about national security, a trade secret, etc.). In such cases, the employer should first try to delete, anonymise or pseudonymise the data that is not to be shared with the employee the rest of the emails requested; it is only if such measures would be insufficient that the employer can refuse to communicate the emails (while still providing to the employee with the reasons for denying their request); or 2. only mentioned in other employees' emails: the employer must find a balance between responding to the employee's access request and protecting the rights of other employees. The employer shall therefore (i) ensure that the method used to identify the requested emails does not lead to a disproportionate infringement of other employees' rights, or (ii) require the requestor to clarify their request. It is shall in any case review the content of the relevant emails and assess whether the communication would infringe the rights of any third party. Finally, the CNIL underlines that personal emails of employees are subject to special protection, since employers are prohibited from accessing them. Hence, in case of access requests, the employer shall not review the content of those emails and just communicate them to the requestor, provided that they are either the sender or recipient of such communication.		
CNIL's guidelines on the use of personal data by processors	Pursuant to the GDPR, a processor may only process personal data to which it has access on the documented instructions of the controller, and may not re-use the data on its own behalf or initiative, unless it is required to do so by national or European laws or regulations. A 'personal processor' who re-uses personal data on its own behalf would be qualified as a controller, and could be liable for not having acted in accordance with the instructions of the original controller. The CNIL however clarifies that a controller may, under the following conditions, authorise a processor to re-use personal data on its own behalf; and the processor would then be the controller for this new processing activity:	12 January 2022	CNIL statement (in French)

Development	Summary	Date	Links
	1. The controller must carry out a "compatibility test" before granting its authorisation: thus, it must determine whether further processing of the personal data by the processor would be compatible with the purpose for which the data was initially collected (where such further processing is not based on the consent of the data subject or under national or EU law) 2. It would be unlawful for a controller to grant to a processor a general, prior authorisation for any further processing of personal data. The controller may only grant its authorisation on a case-by-case basis, taking into account of the purposes and characteristics of each processing operation 3. The authorisation of the original controller must be in writing (which can include by electronic means) The CNIL further clarifies the obligations of the parties under the GDPR where further processing of personal data by the processor is authorised: – the original controller must inform the data subjects that their data would be provided to a new controller, for a new purpose, and about their right to object to such further processing. If the processor already holds the contact details of data subjects, the initial controller can delegate this task to the processor – the processor (which would then become controller) is responsible for the compliance of the processing it implements with all the requirements of the GDPR, ie it must ensure that a legitimate purpose and an appropriate legal basis are identified, that the personal data is retained for no longer than necessary, etc		
Draft report of the CNIL regarding the use of "intelligent" or "augmented" video devices in public places	According to the CNIL, there has been a significant increase in the use of "intelligent" or "augmented" video devices in public places. In order to ensure that such devices are used in a way that respect individuals' right to privacy, the CNIL published in January 2022 a draft report on these "intelligent" video devices, which was subject to public consultation until 11 March 2022. "Intelligent" or "augmented" video devices include software	14 January 2022	CNIL statement (in French) CNIL draft report (in French)

Development	Summary	Date	Links
	allowing for the automatic processing of images collected via CCTV cameras. They allow for the extraction of various information from the footage of CCTV cameras, and can be used by different entities, either public or private, in particular in places open to the public or in the street (eg for safety or publicity purposes, etc.). The CNIL's report does not cover biometric recognition devices or the use of video devices in non-public places. The draft report aims at defining what "intelligent" or "augmented" video devices are and their variety of uses, highlighting the ethical and societal stakes of this technology and the risks for the rights and freedoms of individuals, and establishing a legal framework governing how these devices can be implemented in light of the risks they pose. The CNIL's report notably indicates how the principles of data protection laws and regulations (eg identification of a legitimate purpose and of an appropriate legal basis, compliance with data subjects' rights, etc.) shall apply to any entity using "intelligent" video devices. Since the public consultation on the CNIL's draft report has now ended, it is expected that the CNIL will issue a final report in the near future.		
CNIL ends investigations into tech company's processing of health data	In January 2022, the CNIL decided to close its investigations and to end its formal notice against a French tech company which processes health data, ie the test results from patients undergoing COVID-19 lateral flow tests. In October 2021, the CNIL issued a formal notice to the company to bring its activities in compliance with the GDPR within two months, in particular regarding the security of health data processed on behalf of pharmacies. Online and on-site inspections had been carried out by the CNIL, following an anonymous report, and had shown a data breach on the company's database involving over 380,000 data subjects. The database included the data subjects' names, email addresses, mobile phone numbers, dates of birth, test results (positive or negative) and social security numbers.	27 January 2022	CNIL statement (in French)

Development	Summary	Date	Links
	When issuing its formal notice, the CNIL pointed out that, while the company had taken some steps to remedy the data breach, it considered that these steps were insufficient. In January, the CNIL found that the company had proved it had taken sufficient measures to comply with the GDPR by strengthening the security of its processing. In particular it now uses a service provider with a Health Data Hosting certification, it has strengthened its authentication and implemented cryptological processes, and it has extended the use of logs on its servers.		
Publication of CNIL's final frames of reference on commercial management and unpaid debt management	In November 2018, the CNIL launched a public consultation on its draft frames of reference relating to commercial management and unpaid debt management. In February 2022, the CNIL finally released the updated versions of these two frames of reference. The CNIL's frames of reference can be followed by organisations looking to ensure that their personal data processing activities are in compliance with the GDPR and the French Data Protection Act. Although it is not mandatory to comply with the recommendations included in such frames of reference, organisations deviate from the principles set out by the CNIL must be able to justify their decisions to do so. The final frame of reference on commercial management covers the main personal data processing activities that a company may implement in relation to its clients, ie the management of their contracts with customers, the handling of invoices and payments, the management of loyalty programs and satisfaction surveys, after-sale services and the management of customers' complaints, as well as direct marketing operations. In its frame of reference, the CNIL notably explains how personal data can be exchanged with third parties in relation to direct marketing activities, as well as how long customers' personal data may be retained. Following the public consultation that was launched in 2018, the CNIL has also clarified the legal bases that can be used by companies for their various customer-related data	3 February 2022	CNIL statement (in French) Frame of reference on commercial management Frame of reference on unpaid debt management CNIL Q&A

Development	Summary	Date	Links
	processing operations, as well as the cases in which a DPIA is mandatory. The CNIL's frame of reference on unpaid debt management is aimed at organisations (private or public) processing of personal data in relation to unpaid debts from customers/users. The CNIL underlines that, given the effects that such processing activities may have (ie prevent an individual to conclude any further transaction with the relevant entity), specific safeguards must be implemented, namely: (i) providing information to data subjects throughout the various steps of the process, and (ii) ensuring that personal data is retained only for a limited and proportionate time period, in accordance with the timelines specified by the CNIL. For ease, the CNIL has also published a Q&A on its two new frames of reference.		
Priorities of the CNIL for 2022: direct marketing, cloud services and monitoring of employees working remotely	The CNIL can initiate investigations in response to: complaints from data subjects and reports of data breaches, or in relation to the current events. In addition, the CNIL issues every year a list of high-stake topics on which it wishes to focus its investigations. Generally, around a third of the CNIL's investigations relate to the priority topics it has identified for the relevant year. The three priorities identified by the CNIL for its investigations in 2022 are direct marketing, cloud computing and the monitoring of employees working remotely: 1. Direct marketing – the CNIL has published a new frame of reference on "commercial management" early February 2022, which includes (notably) rules about direct marketing. The CNIL will hence conduct investigations on compliance under the GDPR and against the frame of reference, in particular in relation to the sale by data brokers of personal data to be re-used for direct marketing purposes. 2. Monitoring by employers of remote workers – the CNIL underlines that, because of the COVID-19 pandemic, remote working is still widely used by employees. This has led employers to try to monitor the tasks and activities of their	15 February 2022	CNIL statement (in French)

Development	Summary	Date	Links
	employees working remotely. The CNIL has issued several guidelines on the rules that employers must comply with to respect the privacy of remote workers, and will therefore launch investigations to verify employers' practices in relation thereto. 3. Cloud computing technologies – the CNIL underlines that they are increasingly used both by public and private entities. However, cloud services may create risks for personal data, including data breaches or transfers of massive amounts of data outside the European Union. The CNIL will therefore review with particular attention all subjects relating to the relationships between controllers and cloud service providers, including in respect of data transfers.		

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

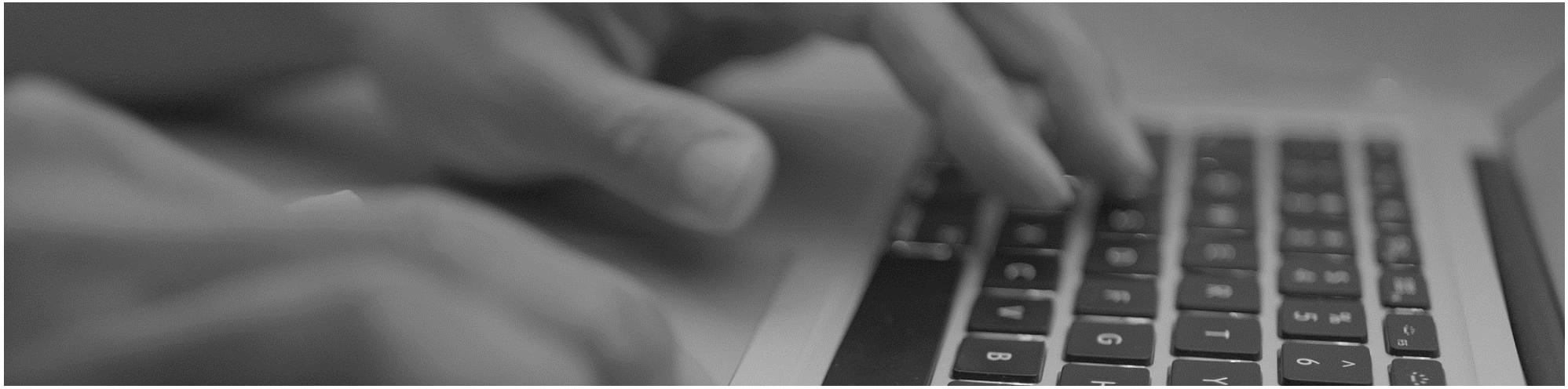
Jeanette da Costa Leite
Associate (PSL)
T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

Development	Summary	Date	Links
Requirements for the secure and data-protection-compliant communication via fax	In a new working paper, the Supervisory Authority of Bavaria states that there are significant risks to data confidentiality in the transmission of personal data via fax at the stages of dispatch, transfer and reception. In a case-specific illustration it is demonstrated that by observing the listed risk scenarios and complying with specific accountability obligations, data protection-compliant transmission via fax can be ensured.	1 February 2022	Working paper (German only)

Development	Summary	Date	Links
Recommendations for actions on information security for IoT infrastructures in smart cities and regions	Many cities and communities are building on the digitalization of essential processes of urban life. By utilising IoT (internet of things) technology, areas such as; mobility; transportation; energy; logistics; health; the environment; and traffic, are to be digitalized, which can make these cities and communities vulnerable to cyber attacks. The Federal Office for Information Securities' recommendations are intended to make it easier to deal with these threats and to ensure the security of data platforms and sources in IoT infrastructures.	17 January 2022	Recommendations (German only)
COVID-19 contact records to be deleted or destroyed immediately after the legal obligation to collect contact data has ceased to apply	As soon as the obligation to collect contact data ceases to apply under state law, obligated businesses and institutions must immediately destroy or delete the contact records completely and irrevocably. In particular, restaurants, cafés and leisure facilities shall ensure that no such personal data is held at all after expiry of the statutory storage period. According to the statement of the Supervisory Authority of Brandenburg ('**SA Brandenburg**'), hospitals, preventive care, rehabilitation facilities and nursing homes are still obliged to record the contact data of guests, customers and visitors. However, they are obliged to delete these records after a four-week period.	22 February 2022	Press statement (German only)
Processing employee personal data on the legal basis of legitimate interest	According to the High Regional Court Brandenburg ("**OLG Brandenburg**"), a legitimate interest pursuant to Article 6(1)(f) GDPR exists if the data processing serves to verify compliance with the obligation to pay the minimum wage to an employee by a subcontractor. However, further information that is contained in a payslip would not be covered by such Article.	23 February 2022	Judgment (German only)
€1.9M fine for unlawful processing of personal data	The Supervisory Authority for Bremen imposed a fine of EUR 1,9 million on a local building association for processing personal data of more than 9,500 prospective tenants pursuant to Article 83 GDPR. The company's unlawful processing included, information on race, ethnic origin, religion sexual orientation and health. Considering the extraordinary severity of the violation of provisions of the GDPR, a significantly higher fine would have	3 March 2022	Press statement (German only)

Development	Summary	Date	Links
	been imposed, if the company had not cooperated comprehensively.		
New FAQs on the processing of employees' personal data in connection with the COVID-19 pandemic published by the DSK	The conference of the independent data protection authorities of the Federation and the Länder published an FAQs concerning the processing of special categories of employees' personal data in connection with the pandemic. The FAQs aim to ensure a nationwide and cross-state uniform application of law in the context of employee data protection during the fight against COVID-19.	7 January 2022	Statement (German only)
Updated version of the BSI Basic IT Protection compendium	The Federal Office for Information Security published comprehensive recommendations on handling threats in the information security sector. These guidelines particularly cover protection measures for networks and data, the set up of information security management systems and guidance on protecting sensitive data.	8 February 2022	Statement (German only)
The right of access and the right to obtain copy of personal data are separate rights under GDPR	The District Court Cologne has ruled that the right of data subjects to obtain a copy of their personal data pursuant to Article 15(3) GDPR is independent from the right of access pursuant to Article 15(1) GDPR. Article 15(3) GDPR constitutes an independent right to obtain a copy of the raw version of the personal data processed.	16 February 2022	Judgment (German only)
New FAQs on cookies and tracking published by the Supervisory Authority Baden-Wuerttemberg	The Supervisory Authority Baden-Wuerttemberg published an updated FAQs catalogue for cookie and tracking implementations by website operators and smartphone app manufacturers. The FAQs provide information on data protection-compliant websites and app solutions to help website operators and app manufactures avoid falling foul of the rules when deploying cookies and tracking software.	4 March 2022	Statement (German only)
New FAQs from Supervisory Authority of Saxonia regarding privacy law aspects of vaccination obligation in the healthcare sector	The Supervisory Authority for Saxonia ("**SA Saxonia**") published a new FAQs regarding mandatory data protection provisions in relation to vaccination obligations of staff in hospitals, practices, care facilities etc., which applied from 15 March 2022. The SA Saxonia analyses the processing of staff members' vaccination	3 March 2022	Statement (German only)

Development	Summary	Date	Links
	status from a data protection perspective and provides recommendations for action.		



Hong Kong

Contributors

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

Jennifer Van Dale
Partner
T: +852 2186 4945
jennifervandale@
eversheds-sutherland.com

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

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

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

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

Hilary Chan
Trainee Solicitor
hilarychan@
eversheds-sutherland.com

Kevin Chan
Trainee Solicitor
kevinchan@
eversheds-sutherland.com

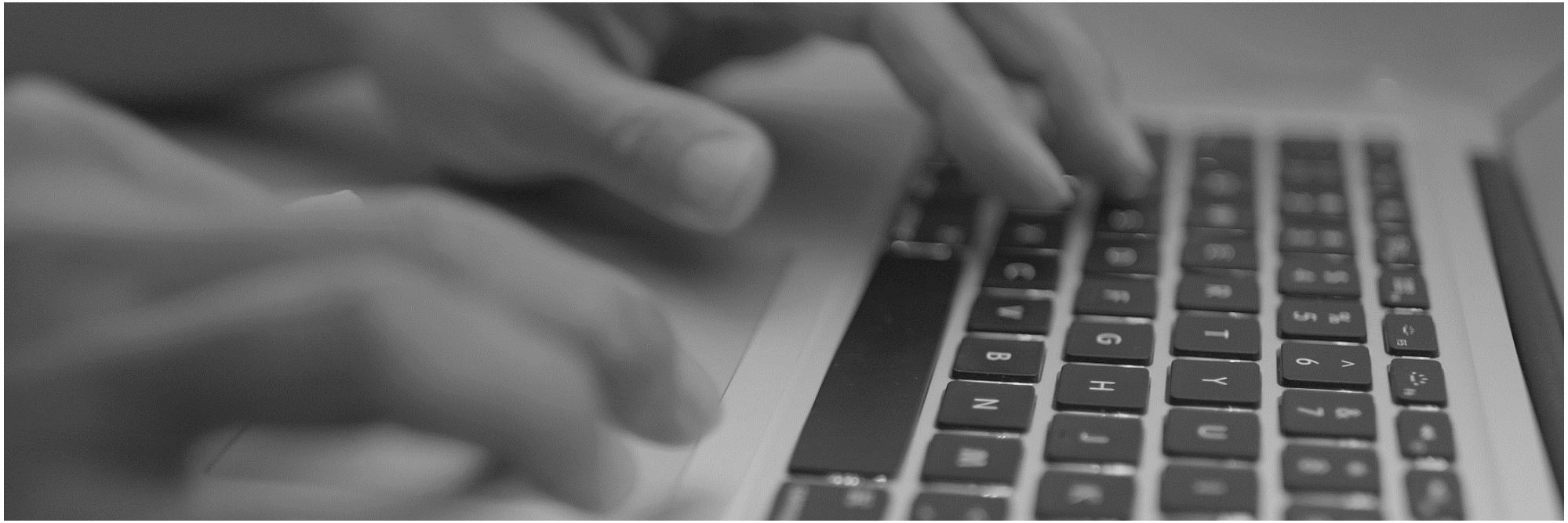
Justina Choi
Trainee Solicitor
justinachoi@
eversheds-sutherland.com

Development	Summary	Date	Links
PCPD publishes investigation report on the incident of the hacking of Nikkei China (Hong Kong) emails	The Office of the Privacy Commissioner for Personal Data ("**PCPD**") published its investigation report into the hacker's email intrusion incident of Nikkei China (Hong Kong) Limited ("**Nikkei**") on 17 February 2022. This investigation arose from a data breach notification lodged by Nikkei on 17 March 2021 which reported that a hacker had gained access to six staff email	17 February 2022	PCPD Investigation Report

Development	Summary	Date	Links
	accounts, forwarding emails that had been sent to those accounts to two unknown email addresses, which resulted in the disclosure of the personal data of over 1,600 customers. The Privacy Commissioner found four major deficiencies in the security of Nikkei's email system: 1. weak password management; 2. retention of obsolete email accounts; 3. lack of security controls for remote access to the email system; and 4. inadequate security controls on the information system. The Privacy Commissioner concluded that Nikkei had contravened Data Protection Principle 4(1) in relation to the security of personal data under the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) ("**PDPO**") (ie it failed to take all practicable steps to ensure that its customers' personal data was protected against unauthorised or accidental access, processing or use), and issued an enforcement notice to direct Nikkei to remedy and prevent recurrence. In the recommendations, the Privacy Commissioner reminded organisations with an email system containing customers' personal data to have in place adequate policies, measures and procedures covering the following areas: 1. establishing a Personal Data Privacy Management Programme; 2. appointing Data Protection Officer(s); 3. devising a policy on email communications; 4. adequate security measures; and 5. instiling a privacy-friendly culture in the workplace.		
PCPD issued guidance for employers on collection and use of	During the COVID-19 pandemic, especially since the onset of the fifth wave in early 2022, organisations in Hong Kong have been deploying prevention and control measures in the workplace to ensure the health and safety of employees. Health data of	25 March 2022	Guidance for Employers on Collection and Use of Personal Data of

Development	Summary	Date	Links
personal data of employees during the fifth wave	employees is normally collected by employers, with a view to introduce effective anti-epidemic measures to reduce the risk of transmission of coronavirus variants in the workplace. With this in mind, the PCPD issued the "Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic" to help employers and employees understand the employers' obligations under the PDPO when it comes to the collection and use of employees' health data in the context of the COVID-19 pandemic. In particular, the guidance provided the following recommendations: 1. Necessity: Employers should only collect health data that is necessary for and directly related to the purpose(s) of data collection. Personal data irrelevant to or not strictly necessary for the prevention or control of COVID-19 in the workplace should not be collected; 2. Data minimisation: The data collected by employers should be adequate but not excessive in relation to the purpose(s) for which it is collected. The least privacy intrusive measures should be adopted; 3. Transparency: Employers should clearly convey all the requisite information to employees, such as by presenting a Personal Information Collection Statement; 4. Retention and erasure: Employers should not retain the health data of employees for a period longer than necessary. When the purpose of collection is fulfilled, the employer should permanently destroy that data; 5. Accuracy: Employers should ensure that policies and systems are in place to maintain accurate and up-to-date vaccination information and test results of employees; and – Security: Employers should take all practicable steps to protect the health data collected against unauthorised or accidental access, processing, erasure, loss or use, including by locking paper records, encrypting electronic records, and		Employees during COVID-19 Pandemic PCPD Media Statement

Development	Summary	Date	Links
	limiting data access to authorised personnel on a need-to-know basis.		



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
Hungarian DPA finds use of facial recognition cameras in public area surveillance systems to be unlawful	The Hungarian National Authority for Data Protection and Freedom of Information ("**DPA**") was informed that the Municipality of Siófok intends to install a 39-camera system with facial recognition artificial intelligence on Petőfi promenade to monitor public space. The Siófok Joint Municipality Office and the Siófok Police Station submitted to the DPA that the justification for the use of AI is that thousands of people visit the nightclubs during the summer period and this has led to a drastic increase in the number of crimes and offences. According to the Mayor's statement, the surveillance system is not linked to any database, the data is not transferred to any other database andit is only stored in the camera system. According to the declarations of the controllers, the processor and the manufacturer of the camera system, the camera system is equipped with facial recognition AI. At present, the DPA has concluded that the application of facial recognition AI has not been implemented by any customer so far. However, the DPA drew the attention of the three organisations to the fact that the current legislation does not allow for the	14 February 2022	Decision No 963-10/2022

Development	Summary	Date	Links
	operation of a public area surveillance system in Hungary that processes biometric data. It should be stressed that the mere fact that a law provides a legal basis for processing does not mean that processing is lawful if it does not respect the requirements of necessity and proportionality. Within the scope of personal data, the assessment of necessity and proportionality requires particular care when processing biometric data as special categories of data, since the processing of biometric data in itself entails a serious restriction of the data subject's right to self-determination of personal data. The processing of data must be proportionate against the severe restriction of rights and proportionate to the purpose of the processing. In responding to the DPA's justificiation for AI, the Joint Municipality Office attached a press release from the Budapest Chief Prosecutor's Office, which reports on the indictment relating to the preparation of the commission of a terrorist act which would have affected the promenade in Siófok. The DPA does not dispute this, but points out that in this case the law enforcement authorities prevented the crime in the investigation phase without using the AI-equipped facial recognition camera system installed on the promenade. In respect of the Joint Municipality Office and Police Office, the DPA finds that the way in which data is processed in the context of the CCTV system is unlawful due to the absence of an agreement between the joint controllers on the allocation of their responsibilities for data processing and the breach of data security and accountability requirements. In relation to the above infringing activities of the manufacturer of the camera system, the DPA does not consider it proportionate and sufficient to establish the mere fact of illegality. In the light of all the circumstances of the case, the DPA has decided that in order to protect personal data in the future, it is necessary to impose a data protection fine of HUF 500,000.00 on the manufacturer of the camera system.		

Ireland

Contributors

Marie McGinley
Partner

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

Leona Chow
Associate

T: +35 31 66 44 25 8
leonachow@
eversheds-sutherland.com

Sophie Delaney
Associate

T: +35 31 66 44 36 5
sophiedelaney@
eversheds-sutherland.ie

Development	Summary	Date	Links
DPC publishes guidance on the supervision of personal data in the courts and certain statutory bodies exercising decision making functions	The Irish Data Protection Commission ("**DPC**") has published guidance on the supervision of personal data in the courts and certain statutory bodies exercising decision making functions. The guidance provides clarity on the scope of the DPC's authority in the context of the processing of personal data by the Irish courts when acting in their judicial capacity. The DPC notes that while it will carefully consider the particular circumstances of any given case, the DPC's general approach to complaints concerning personal data processed in the context of the complaint handling, investigative and/or decision-making functions of statutory bodies, is that it will not examine data protection issues relating to material that is before such a statutory body while there is any ongoing complaint handling, investigative and/or decision-making process. Where such a statutory process is ongoing, any concern or complaint relating to a dispute as to the admissibility, veracity, accuracy, or source, amongst other things, of the personal data that is contained in material put before the statutory body in question, should be raised directly with that statutory body in the first instance. The guidance notes that while the DPC could ultimately find	1 January 2022	DPC Press Release DPC Guidance Note

Development	Summary	Date	Links
	infringements of the GDPR by a statutory body or any party to the complaint handling, investigative and/or decision-making process in question, in such an event, the DPC has no jurisdiction to interfere with the findings of such a body. The full press release and the guidance note are available at the links provided.		
DPC Publishes Guidance on the Data Protection Considerations Relating to Multi-Unit Developments and Owners' Management Companies	The DPC has published guidance which sets out general advice on common data protection issues which may arise in respect of multi-unit developments ("**MUDs**") and owners' management companies ("**OMCs**"). OMCs process and transmit data in the exercise of their functions in relation to, for example, property title, financial management, and compliance with various legal obligations. The guidance sets out general advice on common data protection issues which may arise in the course of interactions between: 1. OMCs and their members; 2. OMCs, OMC members, and a property management agent; and 3. OMCs and third parties. The full guidance is available at the link provided.	1 January 2022	DPC Guidance Note
DPC decision on its Inquiry into a Consultancy Provider	The DPC has published its decision in respect of an Inquiry that was commenced following a personal data breach where a Consultancy Provider sent an unencrypted USB storage device, containing personal data to the controller. The Inquiry considered whether the Consultancy Provider had complied with its obligation to implement an appropriate level of security under Article 32 GDPR. The decision found that the Consultancy Provider had infringed Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data.	24 January 2022	DPC Decision

Development	Summary	Date	Links
	The decision issued the Consultancy Provider with a reprimand in respect of the infringement.		
DPC decision on its Inquiry into Slane Credit Union	The DPC has published its decision in respect of an Inquiry that was commenced in relation to a personal data breach notified by Slane Credit Union to the DPC on 30 November 2018. The personal data breach related to an unauthorised disclosure of personal data in the form of an unintended publication of member data on the internet. The decision found infringements of the following provisions of the GDPR: – Article 5(1)(f) and 32(1) were infringed by Slane Credit Union by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of the personal data of its members; – Article 24 and 30(1) were infringed by Slane Credit Union by failing to implement organisational measures that took account of the nature, scope, context and purposes of its processing, and by failing to include all appropriate information in its record of processing; and – Article 28(1) and (3) were infringed by Slane Credit Union by failing to conduct due diligence on its processor and by failing to put in place an agreement with its processor that met the requirements of Article 28(3) of the GDPR. The decision imposed an administrative fine on Slane Credit Union in the amount of €5,000 in respect of the infringement of Article 5(1)(f) of the GDPR (principle of security of processing). The decision also issued Slane Credit Union with a reprimand in respect of all of the infringements.	26 January 2022	DPC Decision
DPC welcomes National Digital Strategy	The DPC and a number of other bodies have welcomed the publication of the National Digital Strategy by the Government of Ireland. The National Digital Strategy marks a step change for Ireland's ambition to harness the possibilities of digital technology	1 February 2022	DPC Press Release National Digital Strategy

Development	Summary	Date	Links
	for day to day life while providing protection from harm in the online world. The new National Digital Strategy places a particular emphasis on cyber security, and commits to reviewing the National Cyber Security Strategy in 2022, to recognise progress made and to respond effectively to an evolving landscape. Helen Dixon, Ireland's Data Protection Commissioner, commented as follows: "There are many positive aspects to the technology sector's innovative culture that we can learn from. In order to ensure effective regulation, regulators need to ensure that we can hire people with the ability and flexibility to rise to the challenge. We welcome the Government's support to ensure that we attract and retain the talent necessary for this change." The full press release and the National Digital Strategy are available at the links provided.		
DPC publishes blog on "Children and data protection: Reflections on Safer Internet Day"	In a blog post published by the DPC to mark Safer Internet Day (an online safety initiative to raise public awareness of the importance of online safety and to encourage a safer internet for all, especially children), the DPC noted that it will continue to prioritise its work on children's data protection issues, as reflected in its 2022-2027 regulatory strategy published late last year. In the coming months the DPC intends to publish a series of guidance materials specifically for children to explain basic principles of data protection and to assist children in exercising their data protection rights. The press release can be found at the link provided.	8 February 2022	DPC Blog Post
DPC publishes 2021 Annual Report	The DPC published its annual report on 24 February 2022. Helen Dixon, Commissioner for Data Protection, commented that "2021 was a year of strong regulatory results from the DPC, in which it delivered impactful and far-reaching outcomes for the protection of individuals' personal data". This is clearly demonstrated in the statistics highlighted in the report.	24 February 2022	DPC Annual Report

Development	Summary	Date	Links
	Some key areas of interest in the DPC annual report include: – 6,549 valid data breach notifications were received by the DPC in 2021. The report provides that 95% of the total recorded breach cases were concluded in 2021. – The DPC received 7,469 queries and 3,419 complaints from individuals in 2021. Common themes ranged from issues such as access requests, fair-processing, direct marketing and the right to be forgotten. In 2021, the DPC concluded 7,081 queries and 3,564 complaints, including 1,884 complaints received prior to 2021. – The annual report features accounts of the outcomes delivered in a number of significant inquires concluded by the DPC. Over the course of 2021, fines and corrective measures were imposed in a number of finalised cases. The full annual report is available at the link provided.		
DPC publishes independent KOSI audit report into resource allocation	On 11 March 2022 the DPC published the final report of the independent KOSI audit of resource allocation at the DPC. The audit reflected on structure, numbers of staff and the efficacy of the current organisational model in light of risks arising from post-GDPR requirements, while also considering how the DPC aligns with the structures of peer and analogous bodies. The scope of the audit included consideration of demands on the DPC in terms of volumes and caseload, the current organisation structural model, resource allocation, gap and any perceived deterioration in the risk model. The full Audit Report is available at the link provided.	11 March 2022	KOSI Audit Report
DPC publishes statistical report on handling of cross-border complaints under GDPR's one-stop-shop (OSS)	The DPC has published a statistical report on the DPC's handling of cross-border complaints under the GDPR's one-stop-shop mechanism. Since 2018, the DPC has received and concluded a significant number of cross-border complaints as the EU/EEA lead supervisory authority for the large number of technology and	15 March 2022	DPC Press Release DPC Report

Development	Summary	Date	Links
	internet platform companies with EU headquarters in Ireland. The DPC's handling of these complaints has been the subject of public commentary. In the interests of accountability, transparency and informed debate, the published report gives an overview of the DPC's cross-border complaint handling processes and the associated statistics, including the number of complaints received, numbers concluded and outcomes achieved. The full report is available at the link provided.		

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

Development	Summary	Date	Links
Spanish hotel fined for illegal processing of passport photographs of (Dutch) hotel guests – close collaboration with the DDPA	Guests of a Spanish hotel were asked to provide their passports for a scan so that they could be identified. According to the hotel, they were obliged to do so by statutory law. A Dutch hotel guest filed a complaint with the Dutch Data Protection Authority ("**DDPA**"). The Spanish Data Protection Authority ("**AEPD**") took on the case and worked closely with the DDPA on this investigation. The AEPD considers it unnecessary to process a photograph of the passport of hotel guests to identify if the hotel guest placing an order in a restaurant is the right hotel guest. To that extent, the AEPD concludes that to store and share such photographs among employees is an excessive use. The hotel could have used less intrusive means to identify hotel guests, such as asking for a room number, in combination with a name. It is interesting to note that the Spanish supervisory authority initially concluded that the hotel had the right to identify hotel guests by means of their passport photograph. The DDPA considered the practice of the Spanish hotel unlawful and filed an objection. The AEPD held that the objection was well-founded.	11 March 2022	DDPA Statement (Dutch)

Development	Summary	Date	Links
	After mutual consultation with the DDPA, the AEPD adjusted its decision.		
Court rules on right of access and abuse of rights	In 2019, the municipality of Ede imposed an 'additional parking tax' on a Dutch citizen, to which the citizen objected. The objection included a request to provide physical copies of the personal data that the municipality processes regarding the data subject. The municipality was sent a 'source document' and an overview of the registered data, with a description of the means by which it was created. The citizen objected stating that the overview was not complete and did not meet the requirements of the right of access under Article 15 GDPR. The first question in this case was whether the objection letter submitted by the citizen constituted a access request under Article 15 GDPR. The second question was whether there was 'an abuse of rights'. First, the Administrative Court ruled that the request, part of which was a notice of objection against an additional parking tax, was a request for access as referred to in Article 15 GDPR based on the following: – the presentation and formulation of the request under a separate heading 'request for access'; – the circumstance that copies of processed personal data had been requested; and – the fact that 'physical statements' had been requested does not mean that there is no GDPR request. Secondly, the court concluded that by submitting the request, in addition to several actions relating to the GDPR, the citizen did not abuse their procedural rights, based on the following: – the court stated that, in general, a successful appeal to the abuse of rights requires serious grounds, for example when rights or powers have been used without a reasonable purpose, when they were used for a purpose other than that for which they were intended or when they are used in bad faith.	9 March 2022	Court Ruling (Dutch)

Development	Summary	Date	Links
	– additionally, an excessive use of facilities provided by the public authorities generally does not by itself constitute an abuse of rights, but this may be the case in combination with other circumstances. – a comparison with another case in which a citizen provoked an additional parking tax at least 40 times. The court found that the other case contrasted with the case being heard, because the citizen in the other case had submitted their access request to five municipalities and the number of requests and procedures was not clear; – the purpose of the request (of whether the municipality of Ede shared data relating to the citizen with other municipalities) and the other actions of the citizen were in accordance with the GDPR. Referring to Recital 63 of the preamble of the GDPR, a data subject has the right to access personal data which has been collected about them, and must be able to exercise this right easily and with a reasonable threshold, in order to be informed of and verify the lawfulness of the processing.		
Dutch Government sets out its policy for digitization	The Dutch Government has set out its policy for digitization for the upcoming period. It is the first time in the Netherlands that the coalition agreement contains a dedicated section on digitization. The Dutch government has expressed that it aims to take advantage of the opportunities that digital transition can offer. The Netherlands wants to play a strong and anticipatory role in shaping the digital transition in such a way that it fits with Dutch values: security, democracy and self-determination. Fundamental rights and public values must be protected and a level economic playing field must be created with fair competition, consumer protection and broad social cooperation. The Dutch government aims to achieve a safe, inclusive and promising digital society for all Dutch citizens, based on four themes: 1. Digital foundation The digital foundation will create the preconditions to shape the other four themes. Crucial preconditions are:	8 March 2022	Letter to the House of Representatives (Dutch)

Development	Summary	Date	Links
	cybersecurity, online identity and control over personal data, privacy, equal treatment, democracy, a strong rule of law, digital autonomy, digital inclusion and digital infrastructure. 2. Digital Government The digital government places citizens and entrepreneurs at the centre. The goals are to deliver assistance to citizens and businesses, be transparent as a government and be a digital partner. 3. Digital society The Dutch government aims to use digitization to make society more innovative, efficient, and inclusive when it comes to education, health, climate and mobility. 4. Digital economy As digital transition comes with opportunities for the economy and society, it is of importance to the Dutch government to make sure that Small and Medium Enterprises (SME's) and the industry lead the way and invest in digital technology.		
Recruitment agency fined for unnecessary processing of identification documentation in relation to the right of access	The Spanish Data Protection Authority ("**AEPD**") has issued a fine of EUR 240,000 to a recruitment agency. The AEPD conducted this investigation after a Dutch citizen notified the DDPA of a potential data breach. The data subject in question had requested access to the processing of their data by the recruitment agency. The agency would only allow access if the data subject would identify themselves by providing a full copy of their identity document and a copy of their insurance card. In addition, a copy of the data subject's recent energy or water bill was also needed to confirm their address. The AEPD considered that the demand for such data was unnecessary for the right of access. Information about the data subject could also be gathered by means of the account details of the data subject that the agency already possessed.	3 March 2022	DDPA Statement (Dutch)

Development	Summary	Date	Links
	Additionally, the AEPD considered that the request for an identification document is an extreme measure, sating that organisations should only request an identity document in exceptional cases, considering the risks of processing such data (such as a ransomware attack or data breach which could lead to identity fraud if such data was compromised).		
Supervisory authorities call for more awareness about online use of internet user data	The four Dutch Supervisory Authorities (the Authority for Consumer and Markets, the DDPA, the Authority for Financial Markets and the Media Authority) have called for increased awareness when it comes to use of data online. In October 2021, the supervisory authorities have set up a collaborative platform called 'Digital Supervisory Authorities' or 'Samenwerkingsplatform Digitale Toezichthouders' ("**SDT**"). The authorities have joined forces to address digital services in their daily practice, and to ensure their activities are well coordinated and carried out properly. As the possibilities of influencing people online is growing rapidly, the supervisory authorities are of the opinion that people are entitled to know what happens with their data 'behind the scenes'. To this end, companies, institutions and public authorities should give clear explanations. The SDT wants to identify how to best protect people against online manipulation or misuse of personal data. As a result of its initiativ, the SDT intends to formulate guidelines which aim to help organisations achieve effective online transparency. The authorities are also currently discussing how they will supervise new EU legislation with regard to digitalization, including the Digital Services Act, the Digital Markets Act, the Data Governance Act and the Artificial Intelligence Act.	2 March 2022	Netherlands Authority for Consumers & Markets Statement (Dutch)
Supreme Court upholds judgment that the right to freedom of expression and information takes precedence over the right to privacy	On 23 June 2020, the Court of Appeal of Amsterdam issued a ruling on the right to erasure (Article 17 GDPR). The judge ruled that the right to freedom of expression and information of a well known search engine and third parties prevails. The ruling denied the request of the applicant to remove a link from the search engine operator's search results to a website containing personal	25 February 2022	Court Ruling (Dutch)

Development	Summary	Date	Links
	data of the applicant relating to a disciplinary measure imposed in the past. The request for erasure was linked to search results relating to the name of the applicant. Searching against the applicant's name brings up a link to a website containing a so-called "black list" of doctors and the "BIG-register number". The BIG-register lists all licensed healthcare professionals ("**HCPs**"). BIG-registered HCPs are subject to disciplinary law and disciplinary measures imposed on these healthcare professional can be found in the BIG-register. The website contains information on a disciplinary measure imposed on the applicant in the past. According to the Court of Appeal, the assessment of the request to erasure should take place on the basis of Article 17 GDPR. The right to privacy of the applicant should be weighed against the right to freedom of information of Google and third parties. The Court of Appeal took into account that the information to which the search results refer to are up-to-date, relevant, factual in nature and not unnecessarily offensive. The Court of Appeal found it relevant that the BIG-register is often not consulted in practice and that the website is not considered an 'official' black-list, but bears a more private character, having regard to the design, name and language. The Court of Appeal concluded that the right to freedom of information prevails over the right to privacy. The Supreme Court upheld the judgment in appeal and ruled that the appeal in cassation has failed. These complaints were related to the application of Article 10 GDPR. The Supreme Court referred to the considerations of the Court of Appeal in which it stated that the application of Article 10 GDPR would not have led to a different outcome.		
DDPA warns personal data should be protected against "doxing"	On 12 July 2021, the DDPA was asked by the Dutch Ministry of Justice and Safety to provide advice on the legislative proposal to change the Dutch Code of Criminal Procedure regarding the criminalisation of obtaining, dissemination or otherwise making available of identifiable personal data for intimidation purposes.	24 January 2022	DDPA Statement (Dutch)

Development	Summary	Date	Links
	"Doxing" involves the disclosure of personal data for the purpose of causing fear, serious nuisance or inconvenience to a specific person. Data that is used for doxing can be derived from government sources such as the Dutch Land Registry Office ("het Kadaster") and the Commercial Register ("het Handelsregister") of the Dutch Chamber of Commerce. Residential addresses of freelancers can be found in the Commercial Register whilst information about property owners, such as names, dates of birth and prices paid for properties can be found in the Land Register. The Dutch government's proposal aims to criminalise doxing. On 24 January 2022, the DDPA issued its advice to the Dutch government. In the advice, the DDPA recognised the need to criminalise doxing because of the severe consequences doxing can have on individuals, and the fact that existing criminal laws do not cover various cases of doxing. The DDPA then underlined the need to also address the different sources of information, which, in combination with other documents, be used for intimidating purposes like doxing.		
Media company fined for creating unnecessary barriers to the exercise of data subject rights	On 14 January 2022, the DDPA issued a fine of EUR 525,000 to a media company relating to a breach under Article 12(2) GDPR. In the period between May 2018 and January 2019, the DDPA received multiple complaints from data subjects regarding the company's policy on access and erasure requests (under Articles 15 and 17 GDPR). The scope of the investigation was limited to requests that were submitted *outside* the secured digital login environment (data subjects who exercised their rights through such requests, did so via an online form on the company's website). The company policy on requests for access or erasure of personal data was as follows: after submitting a request, data subjects were immediately asked to provide a copy of their identification document. Only after submitting proof of identity would the company process such requests. In cases where requests were submitted via the secured login environment, the provision of a copy of an identification document was not considered necessary.	14 January 2022	DDPA Statement (Dutch)

Development	Summary	Date	Links
	According to the company, processing the proof of identity of data subjects was necessary as it was the only way to establish their identity and to prevent information disclosed in response to requests ending up with the wrong person. The DDPA was of the opinion that the exercise of the data subject's rights should be organized in such a way that identification of data subjects must be accomplished in the least intrusive way. To that extent, the DPPA emphasised the importance of the identity of the data subject being subject to the principle of data minimization and taking into account proportionality. The DDPA noted that the processing of identity documents poses a significant risk to the protection of personal data, and suggested that a less intrusive way of establishing the identity of a requestor could be to consider the personal data that the company already processes about that data subject. The DDPA was of the opinion that the company's policy created an unnecessary hurdle in the exercise of data subjects' rights of access and rights to erasure and that the company had breached Article 12(2) GDPR.		
District Court of Gelderland rules on the erasure of special codes in the Central Credit Information System	In this case, the central issue was whether the Dutch Credit Registration Office ("**BKR**") should remove the registered credits in the name of the applicant in the Central Credit Information System ("**CKI**") of BKR. The applicant based its primary request for deletion of all registrations on the fact that the system of credit and debt registration in the CKI is generally in conflict with the GDPR. According to the applicant, the CKI has no legal basis for processing personal data of the applicant in the CKI by BKR. The secondary request is related to erasure of special codes, based on various interests and personal circumstances which should weigh in the applicant's favor. First, the District Court clarified that BKR, as controller, can process personal data in the CKI on the basis of Article 6(1)(f) GDPR. BKR maintains the central credit registry in the	14 January 2022	Court Ruling (Dutch)

Development	Summary	Date	Links
	Netherlands. To that extent, BKR's legitimate interest lies in protecting consumers from excessive lending, problematic debt situations, limiting financial risks and preventing fraud. In conclusion, the BKR is not obliged to erase personal data on the basis of unlawful processing. Secondly, the court considered that BKR's general retention period of five years does not breach Article 5 GDPR in conjunction with Article 17(1) GDPR. The court considered that, although there is no statutory retention period for this type of information, that does not in itself lead to a conflict with the GDPR's storage limitation principle. Consequently, the DDPA ruled that such a retention period is not considered unreasonably onerous. Thirdly, the court considered the processing of data to be adequate with respect to the purpose of the processing; protection of consumers and credit lenders. Fourthly, the court considered the processing of personal data to be transparent and that BKR had fulfilled its obligation to provide information (Article 14 GDPR), with reference to Article 6 of the General Regulation of BKR. Lastly, the court considered the processing of personal data to be *necessary* and referred to prior case law. In relation to the right to object to the processing of personal data under Article 21 GDPR, the applicant requested that the special codes associated with the credit agreements with International Card Services B.V., Santander and ABN AMRO to be removed from the CKI. The applicant presented facts and circumstances relating to his specific situation and argued that the BKR registrations made it impossible to get a business loan and formed an obstacle to the applicant's personal financial future. The applicant argued that BKR's reasons for maintaining the registrations were no longer relevant, as the income and personal situation of applicant had been stable and sufficient for a long time, and that the registrations hindered the applicant's business and personal development. The court considered that it is for the controller to demonstrate		

Development	Summary	Date	Links
	that its interests outweigh the fundamental rights and freedoms of the applicant. BKR had argued that it was not up to BKR to determine the accuracy of the arguments made by applicant with regard to his financial stability (including the circumstances around his housing situation) or that the applicant's financial situation justifies the granting of applicant's request for erasure. The court considered that BKR had not sufficiently demonstrated that it had legitimate grounds for maintaining the special security codes associated with the credit agreements. Consequently, the court held that the interests of credit providers to gain and retain insight into the credit issues experienced by past applicants no longer outweigh the interests of applicants in being released from the restrictions of BKR's special codes registration. The interest of the applicant to have a clean slate at a certain moment in time and to no longer be associated with a history of debts and payment problems, is a substantial one. Therefore, the subsidiary claim for BKR to erase the applicant's special codes in the CKI was granted by the court.		

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
Signing of the UK-Singapore Digital Economy Agreement	The UK and Singapore have signed the UK-Singapore Digital Economy Agreement ("**UKSDEA**") to establish digital trade rules and digital economy collaborations between the two countries. Key features of the UKSDEA include the following: a. the establishment of rules to prevent unjustified restrictions on cross-border data transfers between Singapore and the UK (this will enable the free flow of trusted data between the two countries for business purposes); and b. the prohibition of unjustified data localisation requirements as a condition of market access. The UK and Singapore have also signed a **Memoranda of Understanding** for cybersecurity cooperation. The two countries will collaborate in areas such as Internet of Things ("**IoT**") security, building capacity for responding to cyber security incidents and promoting cyber resilience, to build a secure cyberspace for businesses and consumers. The UKSDEA is not yet in force, but will come into effect once the UK and Singapore have completed their respective domestic ratification procedures.	25 February 2022	Ministry of Trade and Industry's infopage Ministry of Trade and Industry's press release
Finanacial penalties for data breaches to rise from 1 October 2022	The Personal Data Protection Act 2012 of Singapore ("**PDPA**") was amended in 2020 to raise the maximum financial penalty for a data breach to SGD 1 million, or 10% of local annual turnover for organisations whose turnover exceeds SGD 10 million, whichever is higher. The implementation of the increased penalties was temporarily held back due to economic uncertainty	4 March 2022	Speech by Minister of Communications and Information, at the Ministry of Communications and

Development	Summary	Date	Links
	arising from the COVID-19 pandemic. At the Ministry of Communications and Information ("**MCI**") Committee of Supply Debate on 4 March 2022, Mrs Josephine Teo, the Minister for Communications and Information, announced that the increased penalties will take effect from 1 October 2022.		Information Committee of Supply Debate
Review of the Cybersecurity Act 2018 of Singapore and update to the cybersecurity code of practice for critical information infrastructure sectors	The Cyber Security Agency of Singapore ("**CSA**") will be enhancing the cyber resilience of critical information infrastructure ("**CII**") sectors and securing Singapore's cyberspace under two new initiatives. CIIs are computer systems located wholly or partly in Singapore that are necessary for the delivery of essential services in Singapore. Presently, CIIs have been identified from eleven critical sectors, namely: – Aviation – Banking & Finance – Energy – Government – Healthcare – Infocomm – Land Transport – Maritime – Media – Security & Emergency Services – Water The two initiatives by the CSA are as follows: a. review of the Cybersecurity Act 2018 of Singapore ("**CS Act**") in order to: i. update the CS Act for the evolving digital world;	4 March 2022	CSA press release

Development	Summary	Date	Links
	ii. improve Singapore's cybersecurity stance and awareness of threats to Singapore's cyberspace; and iii. support Singapore's digital economy and way of life. The CSA intends to complete its review (which would include stakeholder and public consultations) by 2023. Thereafter, amendments to the CS Act will be proposed. b. update of the cybersecurity code of practice ("**CcoP**") issued by the Commissioner of Cybersecurity so that the CII sectors may better deal with new and emerging threats (eg ransomware and domain-specific risks). The CSA intends to enhance the existing CcoP to achieve the following three objectives: i. help CIIs improve their chances of defending against cyber threat actors using sophisticated threats; ii. allow CIIs to be nimbler in responding to emerging risks in specific domains; and iii. enhance coordinated defences between the government and private sectors to identify, discover and respond to cyber threats and/or attacks in a timely manner.		
Launch of the Data Protection Essentials Programme	The Personal Data Protection Commission ("**PDPC**") and the Info-Communications Media Development Authority have launched the Data Protection Essentials ("**DPE**") programme, which will be made available to Small and Medium Enterprises ("**SMEs**") from 1 April 2022. The DPE programme aims to help SMEs establish basic data protection and security practices to protect their customers' personal data and recover quickly in the event of a data breach. In the event of a data breach under the PDPA, the PDPC may consider an SMEs implementation of the DPE programme as a mitigation factor when considering the appropriate enforcement actions.	4 March 2022	PDPC infopage IMDA infopage

Development	Summary	Date	Links
Publication of the Personal Data Protection Digest 2021	The PDPC has published the Personal Data Protection Digest 2021 ("**PDP Digest 2021**") which highlights the latest data protection-related articles. The PDP Digest 2021 constitutes perspectives from data protection practitioners relating to the latest amendments to the PDPA as well as other topics broadly related to: a. the regulation of data collection, use and disclosure; b. the data protection responsibilities of organisations; and c. the obligations owed by organisations to data subjects. The PDP Digest 2021 aims to provide readers with practical guidance on PDPA compliance (as contributed by the relevant data protection practitioners).	7 March 2022	PDPC PDP Digest 2021
Phone retailer fined by the PDPC in the first case under the PDPA involving egregious misuse of individuals' personal data to activate and re-sell mobile SIM cards for financial benefit in Singapore	The PDPC has imposed a financial penalty of SGD 21,000 on a large singaporean phone retailer This is the first case under the PDPA involving egregious misuse of individuals' personal data to activate and re-sell mobile SIM cards for financial benefit. The PDPC had observed that between January 2020 and November 2020, there were 3,636 Do-Not-Call ("**DNC**") complaints from persons who received specified messages even though their telephone numbers were registered with the DNC register. Further investigations revealed that 1,379 of the messages were sent from 98 mobile SIM cards registered the retailer's sole proprieter. The PDPC initiated investigations under section 50(1) of the PDPA against SPR for suspected breaches of the PDPA. The PDPC's investigations found that the retailer had exploited the mobile SIM card registration process in order to use customers' personal data without their consent to register for additional mobile prepaid SIM cards which customers did not purchase. The retailer admitted this was done to sell illicit mobile SIM cards for extra earnings, and estimated that they had earned approximately SGD 15,000 across three years of selling such illicit mobile SIM cards to anonymous walk-in customers. These illicit mobile SIM cards were then exploited by unknown perpetrators to	10 March 2022	PDPC decision PDPC and SPF joint media release

Development	Summary	Date	Links
	send unsolicited spam and/or scam messages, often in contravention of the DNC provisions under the PDPA. In determining whether the retailer should be required to pay a financial penalty under section 48(j) of the PDPA, the PDPC considered the following aggravating and mitigating factors: a. aggravating factors i. the retailer's breaches of the PDPA were difficult to detect as they included a high degree of planning and pre-meditation to evade detection by the authorities ii. the retailer was entrusted by customers with their personal data for the purpose of registering mobile prepaid SIM cards, and it had abused its trust by misusing personal data iii. the retailer's breaches of the PDPA caused inconvenience to innocent parties, as the illicit mobile SIM cards were used to send unsolicited messages to phone numbers that were registered with the DNC register iv. the retailer financially gained at least SGD 15,000 for the misuse of their customers' personal data. b. mitigating factors i. SPR admitted to liability early in the investigation process, thus reducing the time and resources expended on investigations. Initially, the PDPC's preliminary decision and intention was to impose a financial penalty of SGD 35,000 on SPR. However, having carefully considered all the relevant factors of this case including the representations made by SPR in order to seek a waiver of the imposition of a financial penalty, or in the alternative, for a lower financial penalty, the PDPC reduced the financial penalty to SGD 21,000 on an exceptional basis. As such, this decision should not be taken as setting any precedent for future cases. Along with the PDPC's investigations, the Singapore Police Force		

Development	Summary	Date	Links
	also conducted parallel investigations into possible cheating-related offences as SPR was also suspected to have abused the computer systems holding the customers' personal data in the commission of the offences. Having conducted their investigations, the Singapore Police Force charged SPR in court with two counts of cheating punishable under section 4(3) read with section 11A of the Computer Misuse Act 1993 of Singapore and section 417 of the Penal Code 1871 of Singapore in relation to his alleged misuse of the computer systems.		

Slovakia

Contributors

Jana Sapáková
Counsel
T: + 421 2 3278 6411
jana.sapakova@
Eversheds-sutherland.sk

Daša Derevjaniková
Associate
T: + 421 2 3278 6411
dasa.derevjanikova@
Eversheds-sutherland.sk

Development	Summary	Date	Links
Inspection Plan of the Office for Personal Data Protection of the Slovak Republic for 2022	The Office for Personal Data Protection of the Slovak Republic has published a plan of its audit activities for 2022. The first part of the plan, "Schengen Acquis", focuses on the identification of the state of processing of personal data in the information systems ensuring the practical implementation of the Schengen Acquis on the Slovak Republic and in its embassies. Audits should mainly consist of continuous and ongoing monitoring of the public authorities' ability to ensure secure and lawful processing of personal data in specific information systems used for the internal protection of the Schengen area. The entities to be audited under this part of the plan are, for example, the national part of the Visa Information System, the national part of the Schengen Information System, the Europol National Headquarters and the Customs Information System. The second part of the plan, "Processing activities", focuses on the compliance of personal data processing within the requirements of the GDPR and Act No 18/2018 Coll. on the protection of personal data. In doing so, it reflects on the risks associated with specific processing activities or with the use of new technologies and procedures, particularly with processes capable of significantly affecting the rights and legitimate interests of data subjects. The checks made under this part should focus on be the processing activities of public authorities, the processing activities of local authorities and the processing activities of real estate agencies.	January 2022	Plan

Development	Summary	Date	Links
Slovak Authority fines telecommunications company EUR 40,000 for recruitment and employment related breaches	The Office for Personal Data Protection of the Slovak Republic imposed its third fine on a telecommunications company in the last 3.5 years. This time the fine amounted to EUR 40,000. In the decision, which was issued on 20 December 2021 (in proceedings issued under case number 01339/2021-Os-10), the Office found multiple violations of the GDPR by the company. The company processed personal data of its employees and job applicants which it obtained through evaluation and profiling techniques deployed as part of its job application process (psychodiagnostics, psychometrics). Violations were committed by the company due to processing the personal data: – without an adequate legal basis – without complying with the information obligations under Article 13 of the GDPR – without carrying out a data protection impact assessment – without processing the contract between the controller and the processor – without recording the processing operation in the company's record of processing activities	20 December 2021 (effective on 7 January 2022, enforceable on 24 January 2022)	Decisions of the Office for Personal Data Protection of the Slovak Republic are not published
Inspection Plan of the Office for Personal Data Protection of the Slovak Republic for 2022	The Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as **"the Office"**) has published on its website a plan of its audit activities for 2022. The first part of the plan "SCHENGEN ACQUIS" focuses on the identification of the state of processing of personal data in the information systems ensuring the practical implementation of the so-called Schengen acquis on the territory of the Slovak Republic and in the premises of the embassies of the Slovak Republic. Audits should mainly consist of continuous and ongoing monitoring of the ability of the public authorities to ensure secure and lawful processing of personal data in specific information systems used for the internal protection of the Schengen area. The entities to be audited under this part of the plan are, for example, the national part of the Visa Information System, the	January 2022	https://dataprotection.gov.sk/uoou/sk/content/plan-kontrol-na-rok-2022

Development	Summary	Date	Links
	national part of the Schengen Information System, the Europol National Headquarters, or the Customs Information System. The second part of the plan "PROCESSING ACTIVITIES" is to focus on the compliance of personal data processing with the requirements of the GDPR and Act No 18/2018 Coll. on the protection of personal data. In doing so, it is to reflect the risks associated with specific processing activities or with the use of new technologies and procedures, in particular with processes capable of significantly affecting the rights and legitimate interests of data subjects. The subject of the checks under this part should be the processing activities of public authorities, the processing activities of local authorities and the processing activities of real estate agencies.		
Slovak Authority fined Slovak Telekom, a.s. EUR 40,000	The Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as **"the Office"**) imposed the third fine on Slovak Telekom, a.s. in the last 3,5 years. This time the fine amounted to EUR 40,000. In the decision, which was issued by the Office on 20 December 2021 in the proceeding conducted under the number 01339/2021-Os-10, the Office found multiple violations of the GDPR by the company. The company processed the personal data of its employees and job applicants which were results based on the evaluation and profiling of the data obtained by the survey (psychodiagnostics, psychometrics). Violations were committed by the company due to processing of the data – without an adequate legal basis – without complying with the information obligation under Article 13 of the GDPR – without carrying out a data protection impact assessment – without ensuring of a processing of the contract between the controller and the processor – without recording the processing operation in the records of the processing activities of the control	20 December 2021 (effective on 7th January 2022, enforceable on 24th January 2022)	Decisions of the Office for Personal Data Protection of the Slovak Republic are not published

Sweden

Contributors

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

Sina Amini
Associate
T: +46 8 54 53 22 17
sinaamini@
eversheds-sutherland.se

Development	Summary	Date	Links
Swedish DPA issues administrative fine against Swedish county for security breaches	The Swedish Authority for Privacy Protection (the "**Swedish DPA**") issued an administrative fine of SEK 1.900.000 against Region Uppsala, which is part of the Uppsala county, after finding that the region had not taken appropriate security measures in its handling of special category personal data. The Swedish DPA had received two personal data breach notifications from Region Uppsala. The data breaches concerned special category personal data that was sent without encryption to recipients inside and outside Sweden. Following the data breach notifications, the Swedish DPA initiated investigations of the region, and both the regional board and hospital board. One of the investigations related to special category personal data and social security numbers sent via e-mail. The actual transmission of the e-mails were encrypted, but not the information contained within the e-mails. The relevant emails contained patient data and were sent automatically to the relevant healthcare administrations within the region, and some which were sent manually to researchers and doctors within the region. For the identified failings in this investigation, the Swedish DPA issued an administrative fine of SEK 300.000 against the regional board of the Uppsala Region. The second investigation related to how the University Hospital in Uppsala sent e-mails with patient data to patients and referrers in third countries, ie countries outside the EU. The audit also covered the storage of patient data in the hospital's e-mail server.	27 January 2022	Press statement (in Swedish) Decision (in Swedish) Decision (in Swedish)

Development	Summary	Date	Links
	The investigation found that e-mails sent via the server were only encrypted if certain technical settings were enabled by the recipient. The Swedish DPA therefore concluded that the hospital board utilised a technology which was dependent on e-mail recipients, and that the hospital board could not ensure that the transmission of all e-mails was encrypted. The Swedish DPA also found that the storage of e-mails containing special category personal data on the server provided an insufficient level of protection. For the identified failings, the Swedish DPA issued an administrative fine of SEK 1.600.000 against the hospital board in the Uppsala Region.		
Swedish DPA submits its annual report for 2021 to the Swedish government	The Swedish DPA has submitted its annual report for 2021 to the Swedish government. The report states, among other things, that in 2021 the Swedish DPA received more than 2300 complaints from individuals concerning data protection, and that the past year was largely impacted by the major reform the authority implemented in its complaints and supervision process. The report further states that the Swedish DPA initiated 104 audits, which is twice as many as the year before. The Swedish DPA also issued administrative fees in eight cases totalling SEK 32,500,000. During 2021, the Swedish DPA also initiated a long-term investment in targeted guidance and support for the innovation system - ie organisations, people and networks that drive the creation, dissemination and innovative exploitation of new technology.	22 February 2022	Press statement (in Swedish) Annual report 2021 (in Swedish)
Swedish DPA launches investigations into the use of cloud-based services by the public sector	As part of EDPB's launch of coordinated enforcement on the use of cloud-based services by the public sector, the Swedish DPA has initiated an investigation. In the first instance, the participating supervisory authorities will send out a questionnaire to the selected public bodies. Across the EU, over 80 public bodies will be covered by the survey. The supervisory authorities will then examine the challenges of public bodies complying with GDPR when using cloud-based services, including areas such as; the processes and safeguarding in place	1 March 2022	Press statement (in Swedish)

Development	Summary	Date	Links
	relating to the procurement of cloud services, challenges related to international transfers, the use of complementary security measures and rules governing the relationship between controllers and processors. For Sweden, the aim is to provide the Swedish DPA with increased knowledge about the use of cloud services by the Swedish public sector, in order to develop appropriate national measures in the future. In addition, the results of the national measures taken by all participating supervisory authorities will be aggregated and analysed to provide further insight into the issue. During 2022, the EDPB will publish a report with the results of the analysis.		
Swedish DPA issues an administrative fine against the Swedish Customs due to inadequate security measures	The Swedish DPA has issued an administrative fine of SEK 300.000 against Swedish Customs for failing to implement adequate processes and technical barriers to prevent data on criminal investigations being transferred to the US via cloud-based software. The investigation by the Swedish DPA revealed that some employees, working within the department for criminal investigations at Swedish Customs, had used the software on their company phones. The employees had linked their private accounts to their company phones, which automatically synched the photos and videos taken using the software to the US based service provider. Swedish Customs had stated during the investigation that the use of the software was not permitted within the agency. The Swedish DPA concluded that Swedish Customs was responsible for any personal data processed by the employees, even if company policy prohibited the use of the relevant software. The Swedish DPA further stated that the agency should have implemented adequate processes and technical barriers to prevent data from company phones being copied and transferred to the US based provider.	16 March 2022	Press statement (in Swedish) Decision (in Swedish)

United Kingdom

Contributors

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

Lizzie Charlton
Senior Associate PSL (Data Privacy)
T: +44 20 7919 0826
lizziecharlton@
eversheds-sutherland.com

Development	Summary	Date	Links
Network and Information Systems (EU Exit) (Amendment) Regulations 2021 in force	The Network and Information Systems (EU Exit) (Amendment) Regulations 2021 came into force on 12 January 2022. The Regulations amend the Network and Information Systems Regulations 2018 ("**NIS Regulations**") to move security incident reporting thresholds for digital service providers (in-scope online search engines, online marketplaces and cloud computing services) out of the NIS Regulations and into guidance issued by the Information Commissioner's Office ("**ICO**"). Relevant digital service providers have to notify a security incident to the ICO if it has a substantial impact on the security of their network and information systems. Following a consultation, on 16 December 2021 the ICO updated its incident reporting guidance pages to reflect this change. The guidance sets out a number of revised thresholds to be taken into account when considering whether the impact of an incident is substantial or not. An incident should be reported if at least one of the revised thresholds is met. The guidance also encourages voluntary notifications of incidents that don't meet the thresholds and flags that notification of personal data security breaches may also be required under UK GDPR.	21 December 2021 (NB updated guidance is applicable from 12 January 2022)	ICO guidance
Court of Appeal allows cross-appeal for UK claimant to serve GDPR claim on US-based defendants	In **Soriano v Forensic News LLC and others**, the Court of Appeal allowed a cross-appeal against the High Court's decision not to give permission to serve a claim for breach of the EU GDPR on a defendant out of the jurisdiction. The case comprises useful commentary and clarification on the application of the territorial scope provisions of the EU GDPR. In particular, a US based news	21 December 2021	Judgment

Development	Summary	Date	Links
	website need only solicit a relatively small volume of EU readership to be caught by the "establishment" criterion of Article 3(1) EU GDPR, and the research activities of journalists are capable of amounting to "monitoring" for the purposes of Article 3(2)(b). The EU GDPR applies to the claim because it was brought before the end of the Brexit transition period. The case concerns a British citizen (the claimant) taking legal action against a US publishing company and various journalists based in the US, over the online publication of commentary / material referring to the claimant in unflattering terms. A news website operated by one of the defendants: (i) attracted "more than minimal" readership from the UK; (ii) accepted donations in GBP and Euros; and (iii) accepted UK shipping addresses in respect of its website store. It also operated a subscription platform which invited UK based individuals to subscribe – it was successful in securing three reader subscriptions in GBP and three in Euros. The Court of Appeal disagreed with the High Court's assessment that the claimant's claim for breach of the EU GDPR did not have a real prospect of success to meet the merits test element, required for granting permission to serve a claim on a defendant outside the jurisdiction. The Court of Appeal applied EU case law and regulatory guidance (including the EDPB's Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)) to apply Article 3 EU GDPR to the facts, determining that: – in relation to Article 3(1) EU GDPR – the defendants did more than merely make their journalism accessible over the internet, in that "they intended to make their output available to the UK and EU". The use of the subscription facility amounted to an activity through a "stable arrangement" and – in relation to Article 3(2) EU GDPR – it was arguable that the collection, assembly, analysis and ordering of personal information in the context of writing and publishing an article was "related to" an offer to provide services in the form of		

Development	Summary	Date	Links
	journalistic output and that these activities fell within the meaning of "monitoring". The judge has also invited the Information Commissioner to consider intervening to assist the court.		
Cabinet Office appeals data breach fine it received	The Cabinet Office has appealed a £500,000 fine it received on 2 December 2021 from the ICO, for publishing the postal addresses of celebrities and public figures of the 2020 New Years Honour recipients. The ICO found that the Cabinet Office failed to put in place appropriate technical and organisational measures to protect people's personal information, and prevent the unauthorised disclosure of the data. The data was published online. The Cabinet Office removed the relevant weblink containing the file once they realised the mistake was made. However, the data was available online for two hours and 21 minutes, was accessed 3,872 times and remained available to anyone who had the exact webpage address, because the file was still cached. The Cabinet Office apologised for the breach and a spokesperson has confirmed that they take the ICO's findings "very seriously". However, they declined to comment on any specific aspects of the appeal.	11 January 2022	Statement
UK commences free trade discussions with India, including commitments to facilitate cross-border data flows	The UK and India have started negotiations in respect of a new free trade agreement. The UK government's Strategic Approach paper outlines a number of overall objectives, including to: (i) seek commitments on free and trusted cross-border data flows, prevent unjustified data localisation, and maintain the UK's high standards for personal data protection; (ii) promote online consumer protection and seek necessary business safeguards in digital trade; and (iii) seek commitments to facilitate more efficient and secure international trade through use of digital technologies, including paperless trading. The House of Commons will be considering the government's approach and objectives by way of an inquiry, inviting submissions to its call for evidence. The deadline for submissions was Sunday 13 February 2022.	13 January 2022	Joint statement Policy paper House of Commons inquiry

Development	Summary	Date	Links
Consultation on expansion of scope of NIS Regulations 2018	As part of its National Cyber Strategy 2022, the UK Government is consulting on proposals for legislation to improve the UK's cyber resilience, with a focus on organisations that play an important role in the UK economy such as managed IT service providers. Recognising in particular that IT supply chains can provide a weak point for mass cyber-attack, the proposals include: – measures to amend the NIS Regulations 2018 to bring into scope those digital service providers that provide critical support to essential UK services, in particular IT managed service providers – the creation of a two-tier supervisory regime so that there is proactive supervision of the most critical in scope digital services and reactive supervision of the rest – measures to expand existing incident reporting duties under the NIS Regulations – "future-proofing" of the NIS Regulations so that changes can be made via secondary legislation in order to enable rapid adaptation to changes in threats and to technological developments. If implemented, these proposals will have a significant impact on the IT sector and consequently on contracts for the supply of certain types of IT services. Consultation closes on 10 April 2022.	19 January 2022	Proposal for cyber resilience legislation - consultation details Embedding standards and pathways across cyber profession by 2025 – consultation details Review report
Consultation on embedding standards and pathways across the cyber profession	In March 2021 the UK Cyber Security Council was created as the UK authority on the cyber profession. In connection with the consultation outlined above, the UK Government is now consulting on how to ensure that this Council is properly empowered to embed standards and pathways across the cyber profession during the period from 2022 to 2025. The intention is that the Council will be able to define and recognise cyber security job titles and link them to existing qualifications and certifications to promote cyber security as a recognised profession. Consultation closed on 20 March 2022.	19 January 2022	Press release

Development	Summary	Date	Links
Regulations on immigration exception in force	The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 (the "**Regulations**"), which amend the Data Protection Act 2018 ("**DPA 2018**") to include the relevant safeguards required by Article 23(2) of the UK GDPR, came into force on 31 January 2022. This follows the Court of Appeal case *R (on the application of Open Rights Group and another) v Secretary of State for the Home Department and another (Liberty and another intervening) [2021] EWCA Civ 800*, in which the Court held that Article 23(2) (the "**Immigration Exemption**") contained inadequate safeguards to protect freedoms and was therefore incompatible with the UK GDPR. The Regulations amend the DPA 2018 to: – make it clear that the Immigration Exemption may only be relied on by the Secretary of State and only if there is an immigration exemption policy document in place; and – require that the Secretary of State must decide whether the immigration exemption applies on a case by case basis.	31 January 2022	Regulations Memorandum
Information Commissioner announces major listening exercise regarding working with the ICO	The new Information Commissioner, John Edwards, has announced a "major listening exercise" in order to obtain views directly from businesses, organisations and people about their experience working with the ICO. The aim of this exercise is to find ways to improve the service the ICO offers. The exercise includes a survey and a series of events held across the UK, including events for business, industry and the public sector in February 2022. There are also events planned for civil society, academia and the public, with a particular focus on young people, as well as events held in Scotland, Wales and Northern Ireland to reflect the ICO's UK-wide remit. The consultation closes on 1 May 2022.	28 January 2022	News Your views matter Consultation
New UK data transfer tools come into force and ICO updates international transfer guidance in relation to restricted transfers	The UK's international data transfer agreement ("**IDTA**") and addendum to the EU standard contractual clauses ("**Addendum**") came into force on 21 March 2022 meaning that they can now be considered and used as valid safeguards for transfers of personal data out of the UK.	21 March 2022	ICO guidance: International data transfer agreement and guidance ICO guidance:

Development	Summary	Date	Links
	The IDTA is a new standalone template contract that can be used when making a restricted transfer of personal data to a country outside the UK – it is essentially the UK's equivalent of the new EU standard contractual clauses ("**SCCs**"). By contrast, the Addendum amends the new EU SCCs to work in the context of UK data transfers. Organisations can choose between the two as a potential "appropriate safeguard" for transfers of personal data out of the UK. From **21 September 2022**, any new contract involving a transfer of personal data out of the UK which requires protection by way of standard contractual clauses, must use either the IDTA or Addendum – the *old* EU SCCs will cease to be a valid safeguard for new contracts from this point. The IDTA and Addendum were laid before Parliament on 2 February 2022, alongside a Transitional Provisions document confirming, among other things, that the *old* EU standard contractual clauses remain a valid means of safeguarding transfers of personal data out of the UK made under contracts made on or before 21 September 2022, provided the processing operations that are the subject matter of the contract remain unchanged, until **21 March 2024**. Clients should note that the UK deadlines for implementing the new IDTA or Addendum, where required, do not align with the timeline for the new EU SCCs. Existing contracts using the old EU SCCs must be repapered with the new EU SCCs by 27 December 2022. So, if your existing contract covers restricted transfers of both UK and EU data using SCCs, in order to repaper just the once, the relevant deadline is effectively 27 December 2022. The ICO has also updated its guidance on International transfers after the UK Exit from the EU Implementation Period, providing welcome clarity on the definition of "restricted transfer". According to the guidance, a restricted transfer is made if: – the UK GDPR applies to the processing of personal data which is being transferred; – the personal data is being sent or made accessible to a receiver located in a country outside of the UK; and		International transfers after the UK exit from the EU Implementation Period

Development	Summary	Date	Links
	– the **receiver is legally distinct from the sender** as a separate company, organisation, or individual, which includes transfers to another company within the same corporate group. (The guidance notes that sending personal data to an employee of the sender's organisation will not be a restricted transfer – the restrictions only apply when sending personal data outside the organisation.) In addition, the guidance reflects that while the UK's current transfer rules mirror the EU GDPR approach, the UK has the independence to keep the framework under review. The ICO has also confirmed that it is developing additional tools to support and guide organisations, including: – clause by clause guidance to the IDTA and Addendum – guidance on how to use the IDTA – guidance on transfer risk assessments – further clarifications on international transfers guidance		
Supreme Court upholds ruling that person under criminal investigation and prior to being charged has reasonable expectation of privacy	In **Bloomberg LP v ZXC** the Supreme Court agreed with the Court of Appeal, finding that a person under criminal investigation has, prior to being charged, a reasonable expectation of privacy in respect of information relating to that investigation. The background to the case is that the appellant (a financial reporting corporation) had published an article in 2016 relating to the activities of a company operating in a foreign state for which the respondent's business division was responsible. Those activities had been the subject of a criminal investigation by a UK law enforcement body. Notably, the information cited by the article originated from a confidential Letter of Request sent by the UK law enforcement body to the foreign state. The respondent subsequently brought a claim against the appellant, claiming that he had a reasonable expectation of privacy in respect of the information published in the article, that the appellant had misused his private information and seeking damages and injunctive relief. The court found that generally the "legitimate starting point" is that a person has a reasonable expectation of privacy in a police	16 February 2022	Judgment

Development	Summary	Date	Links
	investigation up to the point of charge but was careful to emphasise that "*whether there is a reasonable expectation of privacy in the relevant information is a fact-specific enquiry which requires the evaluation of all circumstances in the individual case*" and that this starting point is not a legal rule or legal presumption. The Court took a number of factual details from the case into account when drawing its conclusions, including that: – in none of the pre-publication email communications was there any recognition of the highly confidential nature of the letter of request nor was there any assessment of the potential consequences of breaching that confidentiality or any weighing-up of this against the perceived public interest in publication – no-one at Bloomberg involved in publication of the article was aware of just how sensitive the letter of request was and that the editorial process failed to appreciate that the article potentially engaged the respondent's privacy interests – the article did not present "the fruits of an investigation" into the alleged corruption in the foreign state but instead the individual "targets of the UKLEB investigation and the UKLEB's suspicions based on evidence it had gathered"		
UK and Singapore digital trade deal	The UK and Singapore have signed a digital trade deal, heralded as "the most innovative trade agreement ever signed". It covers a wide variety of areas including open and inclusive digital markets, data flows, consumer and business safeguards, digital trading systems, financial services and tech partnerships. Five associated cooperation agreements have also been signed, including one on cybersecurity and one on electronic trade documents and electronic invoicing.	25 February 2022	Statement
Consultations under the Telecommunications (Security) Act 2021	The UK Government is consulting on draft regulations and a code of practice that set out the measures telecoms providers will need to take to comply with their duties under the Telecommunications (Security) Act 2021 to defend networks from cyber threats which could cause network failure or theft of sensitive data.	1 March 2022	Press release Consultation paper Consultation on legal direction to restrict

Development	Summary	Date	Links
	The measures set out in the draft regulations and guidance have been developed by the DCMS with the National Cyber Security Centre. The DCMS' intention is that the proposed regulations and guidance will ensure better security practices within the sector. Under the proposals non-compliance could potentially result in fines of up to 10% of turnover or, for continuing contraventions, £100,000 per day. The consultation closes on 10 May 2022, with the new regulations and code of practice expected to come into force later in 2022. Separately, the UK Government is consulting with telecoms firms, under the Telecommunications (Security) Act 2021 on proposals to control the use of Huawei in UK networks.		Huawei
Personal emails sent from business email account not private or confidential	As an interesting comparator to the ruling in **Bloomberg** the Court of Appeal in **Brake and another v Guy and others**, upheld the finding that the first defendant's employee's use of a business email account to send personal emails did not amount to a misuse of private information or breach of confidence. The background facts of the case are complex, but in summary: – a cottage was jointly acquired by the appellants (as part of a business partnership) for the purposes of operating a wedding and rental accommodation business in relation to which a dispute arose and litigation ensued – a general business enquiries email account had been set up to assist with the operation of the wedding and rental accommodation business serving as the main business email address for the business – this account was used by one of the appellants for her personal purposes – the relevant appellant made no claim of ownership of the domain or email account after her dismissal from the business, until shortly before litigation was commenced – one of the respondents authorised various people to access the enquiries account in relation to the actual or potential litigation against the appellants – these people included	2 March 2022	Judgment

Development	Summary	Date	Links
	lawyers acting for the respondents, a press agent advising the respondents, the appellants' and one of the appellants' ex-business partners The Court of Appeal upheld the judge's initial finding that the appellant did not have a reasonable expectation of privacy in emails that she received on and sent from the enquiries account and found that the judge's finding that the respondents' limited publication to their advisers and to the trustee in bankruptcy and ex-business partner was neither a breach of confidence nor misuse of private information, was open to him. As in Bloomberg this case turned on the facts in establishing whether or not the relevant individual had a reasonable expectation of privacy. Factors relevant to this decision included that the email account was shared with other employees, those others did not use that account for personal correspondence, the password to the account was held in the claimant's capacity as an employee and not in her personal capacity, her personal emails were not stored separately or marked as personal or private and she also had a separate business email account in her own name which she could have used. This case is also a useful reminder that breach of confidence and the tort of misuse of private information are separate causes of action. Although the claimant had pleaded both, she had relied on the same facts and arguments to support each claim and this was not appropriate. To succeed in a claim for misuse of private information the claimant must establish that there is a reasonable expectation of privacy in relation to the information in issue, which will be assessed taking account all the circumstances, then the defendant must fail to establish that any interference with the claimant's right to privacy was justified. To succeed in a claim for breach of confidence three elements are required; the information must have the necessary quality of confidence about it, it must be imparted in circumstances importing an obligation of confidence and there must be unauthorised use of the information to the detriment of the person communicating it.		

Development	Summary	Date	Links
FCA guidance on operational and cyber resilience	The FCA has published a webpage on operational and cyber resilience in the context of the conflict in Ukraine.	March 2022	Webpage
UK Government plans for digital regulation	The UK Government has published a summary of the responses received to its summer 2021 call for views on its Plan for Digital Regulation. Key themes included: – the need for Government to be clear on how it will measure progress and what goods looks like – a need to enhance technical expertise and understanding – a need for a flexible and innovative approach to regulation, with many respondents in favour of outcomes-based regulation – the importance of international cooperation and consistency – the importance of effective, coherent, transparent and accountable regulators – the need for wide engagement with industry, consumers and civil society Following this, the Secretary of State for Digital Culture, Media & Sport wrote to the Digital Regulation Cooperation Forum ("DRCF") to highlight its plans and priorities for the digital regulatory landscape and the DRCF's potential input into these. The letter asks specifically about the opportunities for collaboration in the areas of AI governance, online advertising, implementation of the National Data Strategy, online safety, data and competition policy. The DRCF is comprised of the CMA, ICO, Ofcom and FCA and its role is to drive a joined up approach to digital regulation across the different regulators.	9 March 2022	Policy paper Letter from DCMS
ICO adds accountability and governance chapter to current draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies	The ICO has added a further chapter to its draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies. This chapter considers accountability and governance in respect of anonymisation and advises on appropriate governance approaches/ structures to anonymisation and mitigating the	9 March 2022	ICO consultation

Development	Summary	Date	Links
	associated risks. Guidance on anonymisation assessments appropriate to organisation structures, legislative obligations, the use of safeguarding depending on the purpose of information and the handling of information in respect of third parties are all addressed in this chapter of the ICO's draft guidance. The guidance also states that conducting a data protection impact assessment can help assess, and document, the impact of anonymisation of personal data on a controller's overall risk. The consultation on the overall guidance (not just this newly published chapter on accountability and governance) closes on 16 September 2022.		
Consultation on Online Advertising Programme	The UK Government has announced a consultation on its new Online Advertising Programme ("**OAP**"). The purpose of the OAP is to ensure that the regulatory framework for online advertising keeps pace with the rapid development of digital technologies and protects consumers and businesses alike. The OAP will review the existing regulatory framework for paid-for online advertising, in particular to tackle lack of transparency and accountability across the supply chain. The Government has expressed a desire to move to a model which places responsibility on each actor in the online advertising ecosystem, rather than just focusing on advertisers. It intends to target both harmful content in adverts and harmful placement or targeting of adverts (currently online advertising is not subject to the same level of regulation as other media such as TV or radio) including "influencer advertising". The consultation is intended to gather views on whether the Government's understanding of the online advertising ecosystem is correct and the priority areas and potential options for reform. The OAP will also complement the Online Safety Bill, with the Online Safety Bill imposing obligations on in-scope organisations to deal with fraudulent paid-for advertising and the OAP covering the role of other organisations in the supply chain, as well as harms not necessarily dealt with by the Bill. The consultation, which is a sizeable document and merits close consideration from interested parties, closes on 1 June 2022.	17 March 2022	Consultation

Development	Summary	Date	Links
Online Safety Bill	On 17 March the Online Safety Bill was introduced to the House of Commons, having undergone several changes since it was first published in draft in May 2021. The Bill is intended to create a new regulatory regime to address illegal and harmful online content. It applies to in-scope UK service providers, as well as to in-scope service providers based outside the UK where UK users are affected. It imposes duties of care on providers of user-to-user services (internet services that allow users to upload and share user-generated content) and search engines. The duties of care include requirements to: – undertake risk assessments in respect of users encountering and being harmed by illegal content – take proactive step to identify and remove specified categories of "priority" illegal content including hate crime, harassment and stalking – take proportionate steps to mitigate and manage the risk of harm to individuals posed by other types of illegal content – undertake separate risk assessments in respect of services accessed by children and protect children's online safety – operate systems and processes that allow affected persons to report illegal and harmful content Providers of user-to-user services that are categorised, in supplementary regulations, as Category 1 services (on the basis of user numbers and functionalities) are also subject to enhanced duties to protect adults from content that is legal but harmful (with the scope of such content to be defined in secondary legislation) and to protect content of democratic importance and journalistic content. The Government also announced (as part of the consultation on the OAP – see above) the introduction of a standalone duty to tackle fraudulent advertising into the Online Safety Bill. In-scope providers of search engines and user-to-user services will need to	17 March 2022	Online Safety Bill Announcement (duty to tackle fraudulent online adverts) Announcement (duties to tackle anonymous abuse and enable opt-out of harmful content) Announcement ('cyberflashing')

Development	Summary	Date	Links
	put in place proportionate systems and processes to deal with publication and hosting of paid-for fraudulent advertising. It also announced the addition of two new duties into the Online Safety Bill: – a duty on Category 1 companies to give adults the ability to block people who have not verified their identity on a platform, with the aim of tackling anonymous online abuse or "trolls" – a duty to give users the ability to opt out of seeing harmful content, such as promotion of self-harm and eating disorders and anti-vaccine disinformation as well as provisions to make cyber-flashing a criminal offence. These changes are in addition to the previously announced addition of three communication offences; sending communications that pose a real and substantial risk of causing harm to a likely audience, sending knowingly false communications intended to cause harm to a likely audience and sending communications which convey a threat of death or serious harm. These will reform existing communications offences (currently set out in Section 1 of the Malicious Communications Act 1988 and Section 127 of the Communications Act 2003) in order to make them fit for purpose in today's digital world The new regulatory regime will be enforced by Ofcom, which will also be required to create codes of practice to supplement the legislation. Ofcom will have the power to impose fines of up to the higher of £18 million or 10% of qualifying worldwide revenue for regulatory breaches. There is also the potential for senior managers to be convicted of criminal offences for serious compliance failures.		

United States

Contributors

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

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

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

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

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

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

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

Development	Summary	Date	Links
Nebraska introduces Uniform Data Protection Act	The Nebraska state legislature has introduced a measure to adopt the Uniform Personal Data Protection Act ("the Act"), the model data privacy law put forth by the Uniform Law Commission. The Act has also been introduced in DC and Oklahoma. The Act is self-proclaimed to be more business-friendly than data privacy laws like the CCPA and GDPR. The law would apply to entities conducting business in the state, or those that direct their products to the state and that 1) control data of 50,000 or more state residents, 2) earn 50% or annual revenue from controlling or processing the data and3) is a	20 January 2022	Uniform Data Protection Act

Development	Summary	Date	Links
	processor acting on behalf of a controller that meets the thresholds in (1) or (2), maintains personal data, unless it does so using "compatible data practices." The Act defines "compatibility" broadly, and does not require consent if "reasonable consumers would expect it to occur or if the consumer directly benefits from the practice." Notably, it also lacks the consumer right of deletion. The bill is currently with the Nebraska Legislature Banking, Commerce and Insurance Committee.		
SEC issues proposed rule that could reach cryptocurrency exchanges	The SEC proposed a rule amending and significantly broadening a rule that defines certain terms used in the statutory definition of "exchange" ("**Proposed Rule**"). The Proposed Rule is intended to "better protect investors and enhance cybersecurity by bringing more Alternative Trading Systems that trade Treasuries and other government securities under the regulatory umbrella." If the Proposed Rule is finalised, many entities, including cryptocurrency exchanges and other "communication protocol systems" using decentralised finance ("**DeFi**") technology, could have to register with the SEC and be subject to new reporting and other regulatory, including cybersecurity, requirements (see above). One change would redefine exchanges to include "communication protocol systems that make available for trading any type of security." While the Proposed Rule does not explicitly reference cryptocurrency, other digital assets, DeFi, or related concepts, the Proposed Rule may have been intentionally drafted to subject cryptocurrency exchanges and DeFi platforms to SEC regulation. The Proposed Rule was published to the Federal Register on 18 March 2022. There is a 30 day comment period closing 18 April 2022, after which the SEC will review the comments and prepare a final rule or withdraw the proposed rule. This Proposed Rule is a modified version of a similar rule that the SEC proposed in September 2020.	26 January 2022	SEC Proposes Amendments to Include Significant Treasury Markets Platforms Within Regulation ATS
NIST publishes cybersecurity guidance for internet-of-things devices	The National Institute of Standards and Technology ("**NIST**") published a whitepaper titled "Recommended Criteria for	4 February 2022	Recommended Criteria for Cybersecurity

Development	Summary	Date	Links
	Cybersecurity Labelling for Consumer Internet of Things ("**IoT**") Products" in response to Executive Order 14028, "Improving the Nation's Cybersecurity." The paper contains recommendations for the labelling of consumer IOT products related to the cybersecurity standards they have met effectively, creating a simple label that a consumer without specialised knowledge can look at and quickly ascertain roughly how safe it may be, depending on what it is to be used for. Specifically, NIST recommends that information should exist online for any labelled product, including: – Intent and scope: What the label means and does not mean, including addressing potential misinterpretations; inclusion of a statement that a label does not imply product endorsement by the label programme – Product criteria: What cybersecurity properties are included in the baseline and why and how these were selected; include information on how the criteria address security risks both to the consumer and to others for common intended uses of the products – A glossary of applicable technical terms, written in plain language – General information about conformity assessment: How cybersecurity properties are evaluated – Declaration of conformity: The product's specific declaration of conformity to the baseline criteria, including the date the label was last awarded – Scope: The kinds of products eligible for the label and an easy way for consumers to identify labelled products – Changing applicability: The current state of product labelling as new cybersecurity threats and vulnerabilities emerge – Security considerations for end-of-life IoT products and implications for functionality if the product is no longer connected		Labelling for Consumer Internet of Things (IoT) Products

Development	Summary	Date	Links
	– Expectations for consumers: The responsibility consumers share in securing software and how their actions (or inactions) can impact the software's cybersecurity – Contact information for the labelling programme and information on how consumers can lodge a complaint against a vendor regarding a product label		
SEC proposes cybersecurity risk management rules for investment advisers, funds and business development companies	The SEC proposed a package of new rules and amendments ("**Proposal**") designed to enhance the cybersecurity practices at investment advisers and investment companies, including mutual funds, exchange-traded funds, insurance separate accounts, business development companies and closed-end funds. First, the Proposal sets out new Rule 206-4(9) under the Investment Advisers Act of 1940 and new Rule 38a-2 under the Investment Company Act of 1940 that would require advisers and funds to implement cybersecurity policies and procedures that are tailored based on the adviser or fund's business complexity and cybersecurity risks. Second, the Proposal introduces a requirement for advisers to report "significant" cybersecurity incidents to the SEC within 48 hours, including on behalf of a fund or a private client. Third, the SEC proposes amending existing adviser and fund disclosure requirements. With respect to funds, Form N-1A, as well other fund registration forms, would be amended to require specific prospectus disclosures of significant fund cybersecurity incidents occurring in the prior two fiscal years that affected the fund, the fund's adviser, or the fund's service providers. Likewise, for advisers, the Form ADV Part 2A would be amended to require similar disclosures of cybersecurity risks and incidents. Fourth, the Proposal sets forth new recordkeeping requirements under Advisers Act rule 204-2 and proposed rule 38a-2 under the Investment Company Act of 1940. The comment period will remain open until 11 April 2022, after which the SEC will review the comments and prepare a final rule or withdraw the proposed rule.	9 February 2022	Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Development	Summary	Date	Links
Massachusetts proposes Information Privacy and Security Act	The consumer data law would draw from similar laws like the CCPA. The law would apply to entities 1) doing business in Massachusetts or 2) offering goods or services to, or monitoring the behavior of, residents of Massachusetts, that have $25,000,000 in revenue, and that process the personal data of at least 100,000 residents, or is a data broker. Applicable entities must provide consumers notice that their data is being collected, the purpose for which it is collected, how long it will be retained, and who it may be shared with. Providing notice alone will not authorise the business to proceed with the collection of data; the consumer must affirmatively consent to specific terms. Consumer rights include the rights of notice, deletion, access, correction, obtaining a copy, limiting the use and disclosure of sensitive data, and to opt out of the sale of their data. The Massachusetts law makes special note of data brokers, and requires them to register with the state government. The bill has moved out of the Senate Joint Committee on Advanced Information Technology, the Internet and Cybersecurity, and has been referred to the committee on Senate Ways and Means.	22 February 2022	Massachusetts Information Privacy and Security Act
Utah passes consumer privacy law	Utah passed a consumer privacy law (the Utah Consumer Privacy Act, "**UCPA**"), becoming the fourth state law to create enhanced data privacy rights and protections for consumers. The bill will go into effect on 31 December 2023. While the bill is largely similar to privacy laws in California, Colorado, and Virginia, it is narrower in applicability and scope, and contains more exemptions and fewer corrective mechanisms for consumers. The bill is applicable to: – Organisations that conduct business in Utah – Organisations that 1) create products or services targeted to residents of Utah, 2) have annual revenues of $25,000,000 or more, and 3) control or process personal data of 100,000 or more consumers in a calendar year, **or** derive over 50% of	3 March 2022	Utah Consumer Privacy Act

Development	Summary	Date	Links
	revenue from the sale of personal data, and controls or processes the personal data of 25,000 or more consumers The UCPA gives consumers rights to: – Be informed as to what personal data is collected, how it is used and whether it is sold – Access and delete personal data collected by certain businesses – Obtain a copy of their personal data that has been collected – Opt out of collection, sale and use of their data for certain purposes The UCPA requires certain business entities to: – Safeguard consumer data – Inform consumers as to how their data is used – Comply with consumer requests to exercise their privacy rights		
Rhode Island introduces data privacy bill	A bill introduced into the Rhode Island House of Representatives (Rhode Island Information Privacy Act) (the "Act") would establish consumer privacy rights and requirements for controllers and processors, and a state privacy commission to enforce its regulations. The Act would give consumers the right to access their personal information that was processed by a processor or other firm, know how long it is being stored by the processor, request that their information stop being collected, request that any inaccurate information be corrected, and request that their personal information that has been collected or stored be deleted. The Act would have a low jurisdictional bar, requiring only that it conducts business in Rhode Island, has an annual revenue of $10,000,000 through at least 300 transactions, or processes the personal information of at least 10,000 people per year. The act would allow anyone alleging a violation to bring a complaint to the privacy commission, which could administer a	7 March 2022	Rhode Island Information Privacy Act

Development	Summary	Date	Links
	penalty and would also allow for a private right of action; individuals could choose either one, or both. On 31 March 2022, the House State Government and Elections Committee recommended that the bill be held for further study.		
SEC proposes new cyber incident reporting rules	Paralleling the Cyber Incident Reporting for Critical Infrastructure Act which requires reporting of cyber incidents within the critical infrastructure community, the SEC has proposed rules that would require covered organisations to report, within four business days, any material cybersecurity incidents and the details surrounding them. Under the rules, covered organisations must update the SEC as to previously reported incidents, and when a series of individually immaterial incidents has become material in the aggregate. Entities would also need to disclose their cybersecurity risk management policies, management's role and expertise in managing cybersecurity risks, and the board's oversight into the entity's cybersecurity.	9 March 2022	Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
US Congress passes the Cyber Incident Reporting for Critical Infrastructure Act	As part of a recent push to increase cybersecurity and readiness in the United States, especially given the conflict between Russia and Ukraine, the US government has established new rules governing private entities that fall within one (or more) of the 16 critical infrastructure sectors defined by the Department of Homeland Security. The Act will require entities to report "covered cyber incidents" within 72 hours, and any ransom payments within 24 hours, to the Cybersecurity and Infrastructure Security Agency ("**CISA**"). The definition of a covered cyber incident has not yet been finalised, but must include at least one of the following: – Unauthorised access to an information system or network that leads to loss of confidentiality, integrity, or availability of such information system or network, or has a serious impact on the safety and resiliency of operational systems and processes – Disruption of business or industrial operations due to a denial of service attack, a ransomware attack, or exploitation of a	11 March 2022	Cyber Incident Reporting for Critical Infrastructure Act of 2022

Development	Summary	Date	Links
	zero-day vulnerability, against: (1) an information system or network; or (2) an operational technology system or process – Unauthorised access or disruption of business or industrial operations due to loss of service facilitated through, or caused by a compromise of, a cloud service provider, managed service provider, other third-party data hosting provider, or supply chain attack Entities that are already required to report cyber incidents to other agencies will not be required to submit duplicate reports to CISA; a safe harbour exception will protect entities from any liability they would otherwise incur for sharing information with the government related to the incident. The Director of CISA will have up to 3.5 years from 11 March 2022, to publish a final rule that puts the Act into full effect, although it is possible that the rule is finalised earlier.		
Iowa moves forward with consumer privacy bill	The Iowa House of Representatives passed House File 2506, a bill that, if enacted, would provide for similar consumer privacy protections and requirements as the Utah Consumer Privacy Act. The bill is applicable to: – Organisations that conduct business in Iowa – Organisations that 1) create products or services targeted to residents of Iowa, and 2) – control or process personal data of 100,000 or more consumers in a calendar year – derive over 50% of revenue from the sale of personal data, and controls or processes the personal data of 25,000 or more consumers Note that Iowa does not include a minimum annual revenue requirement. The bill would give consumers the right to: – confirm whether a controller is processing the consumer's personal data and to access such personal data	14 March 2022	Iowa's proposed consumer privacy bill

Development	Summary	Date	Links
	– delete personal data provided by the consumer – obtain a copy of the consumer's personal data, except personal data that is defined as "personal information" pursuant to section 715C.1 that is subject to security breach protection, that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means – opt out of targeted advertising or the sale of personal data Similar to the UCPA, the bill does not provide for a private right of action, allows a 30 day cure period for noncompliant businesses, and does not allow consumers to opt out of profiling, except for targeted advertisements. The bill has been referred to the House Judiciary Committee.		
EU and US reach agreement in principle on preliminary data privacy framework for personal data transfers	The EU and US have reached an "agreement in principle" on a new deal that would allow personal data to flow from the EU to the US – see above.		

For further information, please contact:

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

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

@ESPrivacyLaw

Editorial team

Lizzie Charlton
Senior Associate PSL (Data Privacy)
lizziecharlton@eversheds-sutherland.com

Tom Elliott
Project Co-ordinator
thomaselliott@eversheds-sutherland.com

Shanna Everson
Trainee Solicitor
shannaeverson@eversheds-sutherland.com

Rumaysah Khan
Apprentice Solicitor
rumaysahkhan@eversheds-sutherland.com

Lucy Wainman
Trainee Solicitor
lucywainman2@eversheds-sutherland.com

Olivia Carey
Trainee Solicitor
oliviacarey@eversheds-sutherland.com

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

eversheds-sutherland.com

CAM_1B\7700096\2