EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

January to March 2021

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 2021 and is full of newsworthy items from our team members around the globe. Of note, during that quarter we have seen updates including:

- many jurisdictions continue to provide contact tracing and return-to-work guidance in light of the COVID-19 pandemic.
- many European jurisdictions are clamping down on the use of CCTV in the workplace, and are looking sceptically on the processing of biometric data and the use of Artificial Intelligence.
- in the US, Virginia became the second U.S. state to adopt an enhanced privacy law, and the FTC signalled an increased focus on commercial collection and use of biometric data;
- in Germany, a court decided that the granting of damages under Art. 82 GDPR always requires concrete evidence of the damage suffered by the data subject;
- in the Netherlands, the DDPA has imposed a fine of €475,000 on Booking.com for failure to report a data breach to the DDPA in a timely manner;
- in Russia, new requirements for providing consent to distribution of personal data have been established and fines for infringements of personal data law have been increased;
- in Italy, IDPA issued an emergency measure against a social network imposing an immediate restriction to the processing of data of users whose age could not be established with certainty; and
- in the UK, the head of the Department of Culture, Media and Sport stated that he wants the rhetoric around the use of data to shift from primarily focussing on privacy to focusing more on securing personal information whilst enabling its use to further economic and societal objectives.

We hope you enjoy this edition of Updata.

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

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

Follow us on Twitter at:

@ESPrivacyLaw

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
Senior Associate
T: +43 15 16 20 160
michael.roehsner@
eversheds-sutherland.at

Development	Summary	Date	Links
Austrian Supreme Court requests a preliminary ruling from the CJEU regarding Art. 80 GDPR in a consumer class action	An Austrian consumer protection association has initiated a class action proceeding against a car rental company regarding their use of specific General Terms and Conditions (**GTC**) clauses and other specific clauses covering data processing relative to the customers' use of connected entertainment systems in the rental cars. The Austrian Supreme Court has requested a preliminary ruling from the CJEU on whether competitors or consumer protection bodies are prevented by Article 80 GDPR from bringing class action proceedings against **GTC** clauses for breaches of the GDPR independently from a specific data subject's mandate, based on unfair competition legislation. The CJEU proceeding has case No. C-701/20.	Date of decision: 25 November 2020 Published: 22 January 2021	Austrian Supreme Court Decision (German) Link CJEU proceeding site Link
Federal Administrative Court: names in borough council meeting minutes do not require anonymization before being published	An Austrian borough had to decide on an offer for the purchase of real estate held by the borough. The decision to accept or reject the offer required discussion with the borough council which is required to grant access to its minutes and is allowed to publish them online under the relevant Local Government Act. The potential buyer claimed infringement of their rights under the GDPR and official secrecy, the latter of which is applied rather	Date of Decision: 13 November 2020 Published: 12 February 2021	Link to decision (German) Link

Development	Summary	Date	Links
	deliberately as it is held in high regard by administrative bodies. The potential buyer requested that their name would be anonymized in the published minutes of the council meeting. The **Austrian DPA** and the **Federal Administrative Court** decided that the borough council was empowered by the Local Government Act to publish the potential buyer's full name, supported by legitimate public interest in transparency regarding the subject matter of public real estate property. It was decided that this legal authorization and the aforementioned public interest outweighed the potential buyer's rights.		
Austrian DPA: negative COVID-19 test results may be notified to public health authority	Under the Austrian Epidemic Act any positive test result for any listed disease has to be notified to the health authorities. In July 2020, the Federal Minister for Health Affairs extended this obligation to negative test results for the purpose of pandemic management by public ordinance. A complaint was filed against a private laboratory that notified a negative test result to the public health authority. The **Austrian DPA** agreed with the complainant that a negative test result is considered special category personal data (being data concerning health) and is therefore covered by Article 9 GDPR. However, the **DPA** has ruled that the notification by the private laboratory is covered by the obligation under the public ordinance, wherefore negative test results have to be notified as well.	Date of Decision: 27 October 2020 Published: 25 March 2021	Link to the decision (German) Link
Austrian DPA: Quarterly Report	Quarterly Report by the **Austrian DPA** – in this report, the **DPA** focusses on COVID-19 contact tracing questions and reports (among others) on a decision regarding data processing by election campaigns that has not yet been published.	28 January 2021	Link to the newsletter (in German) Link
Austrian DPA: European Data Protection Day special edition publication	The **Austrian DPA** has issued a special edition publication on the "European Data Protection Day 2021", focussing on data processing in connection to COVID-19 related obligations and medical test data.	28 January 2021	Link to the publication (German) Link

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

Jerry Wang
Senior Associate
T: +86 21 61 37 1003
jerrywang@
eversheds-sutherland.com

Development	Summary	Date	Links
Information Security Technology – Guidelines for the Categorisation and Classification of Information Security Incidents (the "Guidelines")《信息安全技术 信息安全事件分类分级指南》	On 22 January 2021, the State Administration of Market Regulation and the Standardization Administration of China released a draft of the updated Guidelines. Once the **Guidelines** are finalised and come into effect, they will replace the existing guidelines (ie. GB/Z 20986-2007), which have been in effect since 2007. The main changes from the previous published version of the **Guidelines** include: 1) upgrading the legal status of the document from "Technical Guidance (GB/Z)" to "Recommended National Standard (GB/T)", 2) increasing the number of categories of information security incidents from seven to eight, 3) supplementing and improving the terms and definitions, 4) adding descriptions for the three gradings on the importance of information systems, 5) amending the rules for classification of information security incidents in terms of severity, and 6) adding an appendix which defines each of the eight categories in relation to each of the four classifications. The **Guidelines** provide guidance for categorisation and classification of information security incidents in order to prevent the consequences of improper handling of data security incidents,	22 January 2021	Information Security Technology – Guidelines for the Category and Classification of Information Security Incidents Link

Development	Summary	Date	Links
	and to reduce the risks and losses caused by untimely or poorly-analysed responses to data security incidents. The classification of information security incidents mainly takes into account three factors: 1) the importance of the information system concerned, 2) the consequential system loss, and 3) the social impact. Information security incidents are divided into the following eight categories: malware incidents, network attack incidents, data attack incidents, harmful content incidents, facilities faults incidents, illegal operation incidents, force majeure incidents and other incidents. Information security incidents are classified into four different levels in descending severity: Extraordinary Incident (Level 1), Major Incident (Level 2), Significant Incident (Level 3), and Ordinary Incident (Level 4).		
"Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications" **《常见类型移动互联网应用程序必要个人信息范围规定》**	On 12 March 2021, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security and the National General Administration of Market Supervision and Administration jointly promulgated the "Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications"《常见类型移动互联网应用程序必要个人信息范围规定》(the "**Provisions**"), in order to implement the provisions of Cybersecurity Law of the PRC. The **Provisions** clearly state that mobile application ("App") operators shall not refuse provision of any basic services to customers if they refuse to provide unnecessary personal data. Common types of Apps are divided into 29 different categories, and the scope of "necessary personal information" for each category is clearly defined. Provincial and municipal governments and their relevant departments are asked to supervise App operators in their regions to implement the Provisions, to strengthen supervision and monitoring of App operators, and to deal with the illegal	Published: 12 March 2021 Effective Date: 1 May 2021	Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications Link

Development	Summary	Date	Links
	collection and use of personal information, in order to safeguard the legitimate rights and interests of citizens in the cyberspace. Applications covered by the **Provisions** include those pre-installed and downloaded Apps on mobile intelligent terminals, as well as Apps that are usable without pre-installation or downloading.		

France

Contributors

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

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

Camille Larreur
Associate
T: +33 1 55 73 41 25
camillelarreur@
eversheds-sutherland.com

Nastassia Château
Associate
T: +33 1 55 73 41 34
nastassiachateaux@
eversheds-sutherland.com

Development	Summary	Date	Links
The CNIL publishes a practical guide on data pairing with the National Health Data System based on the national insurance number	The **CNIL** intends to help scientists wishing to work with data from the National Health Data System ("**SNDS**") to implement a pairing circuit that complies with security requirements. Pairing is the matching of distinct data sets, using common information (for example, the grouping of patient data from different sources). The **CNIL** has been supervising health data matching with the National inter-regime health insurance information system (SNIIRAM) and **SNDS** for many years. Processing involving the use of the national insurance number ("**NIR**") as a key identifier for deterministic pairing of health data with the **SNDS** requires particular attention. In this context, various types of third parties may be involved in the pairing circuits and participate in their security: for the centralisation of data, for the reconstruction of the **NIR** from the identity traits and, sometimes, for the formatting of identity files. The guidelines present the most common circuits which comply with legal obligations and have been validated by the **CNIL**, and also present the criteria that should lead to the use of an independent third party in order to partition the pairing data, as well as the criteria for ensuring the independence of this third party.	8 January 2021	CNIL's Guidelines (in French) Link CNIL's Statement (in French) Link

Development	Summary	Date	Links
The CNIL publishes the results of the survey and public consultation on the Digital Rights of Minors	The **CNIL** is currently conducting a comprehensive study on the protection of minors' personal data and in particular on the exercise of their digital rights. The aim is to propose practical advice and to clarify certain aspects of the legal framework in order to better protect the rights of minors in the digital environment. In particular, the study found that: – Surfing the internet without parental intervention is widespread – Young internet users are going online earlier and earlier; – Parents prefer activity monitoring solutions rather than prohibition – Internet use by minors is underestimated by parents Several questions remain unanswered: verification of age and consent, the conditions under which minors can perform certain acts on the internet alone, and the criteria for minors to exercise their rights relating to their personal data. The **CNIL** will publish all its conclusions on these various points during the first half of 2021.	11 January 2021	CNIL's statement (in French) Link
The CNIL issues a decision against the Ministry of the Interior for the use of drones	On 12 January 2021, the **CNIL** ruled against the Ministry of the Interior for the unlawful use of drones equipped with cameras, in particular to monitor compliance with lockdown measures. It ordered the Ministry to cease all drone flights until a legal framework authorises them. The French Data Protection Act provides that processing implemented by the State, in particular to prevent or detect criminal offences, carry out investigations or protect against public security breaches, must be provided for by a legislative or regulatory text. In addition, an impact assessment must be carried out when these processing operations present a high risk to the rights and freedoms of individuals. However, to date, no text authorises the Ministry of the Interior to use drones equipped with cameras capturing images in which people are identifiable. Similarly, although it is mandatory, no	Date of CNIL's decision against the Ministry of Interior: 11 January 2021 Date of CNIL's statement: 14 January 2021	CNIL's decision against the Ministry of Interior (in French) Link CNIL's statement (in French) Link

Development	Summary	Date	Links
	impact analysis has been communicated to the **CNIL** concerning the use of these drones. Nor was the public informed of the use of drones as it should have been. Furthermore, although the Ministry of the Interior states that it has developed a mechanism to blur individual's images, this mechanism was not implemented until August 2020, when many flights had already been carried out. Moreover, this mechanism cannot be executed directly by the drone. Images containing personal data are therefore collected, transmitted and processed by the Ministry of the Interior before this blurring system is applied. Finally, this mechanism does not necessarily prevent the identification of individuals as long as the services of the Ministry of the Interior are able to deactivate the blurring. The **CNIL** issued a reminder to the Ministry of the Interior since it cannot impose penalties on the State. In addition to this sanction, the **CNIL** ordered the Ministry to cease, without delay, all use of drones until a legal framework authorises such processing of personal data.		
The CNIL issues its second opinion on the tools and files put in place by the Government in the fight against the COVID-19 pandemic.	The SI-DEP file is a national information system implemented by the Ministry of Solidarity and Health which centralises the results of SARS-CoV-2 tests carried out by public or private laboratories and certain authorised health professionals. The lawmaker wished to regulate this processing, which includes numerous personal data, including health data. This is the **CNIL's** second opinion on SI-DEP. The **CNIL** noted that the remarks made at the end of the first inspection phase in September 2020 had been taken into account. It also noted a satisfactory level of compliance with data retention periods. The CNIL considers that the conditions for implementing SI-DEP do not call for any particular measures on its part. The Contact COVID processing implemented by the National Health Insurance Fund ("**CNAM**") collects information on contact cases and contamination chains. It aims to detect contact cases at three different levels. The **CNIL** found that the processing carried out by the **CNAM** had certain residual bad practices relating to authentication conditions, traceability and the transmission of personal data to a third party not authorised to	Date of CNIL's opinion: 11 January 2021 Date of CNIL's statement: 21 January 2021	CNIL's opinion (in French) Link CNIL's statement (in French) Link

Development	Summary	Date	Links
	host health data. With regard to the processing carried out by a Regional Health Agency ("**ARS**"), although the **CNIL** noted the implementation of numerous measures to guarantee optimal respect for personal data, it also noted several shortcomings in another **ARS** in the management of data, particularly concerning their retention period and security. The **CNIL** informed the **CNAM** and the **ARS** concerned of its findings and warned that further control could take place.		
The CNIL issues an opinion on the proposed "global security" law	The draft law on global security contains several provisions that are directly relevant to data protection (e.g. video protection and drones). In its opinion of 26 January 2021, the **CNIL** emphasised the ethical implications of deploying tools that present risks to civil liberties and privacy. It thus warns against mobile devices, which are discreet by nature, and when held high, make it possible to film places that were previously difficult to access (or even forbidden) for conventional cameras. The image capture that they allow is considerably extended and, above all, can be individualised with the tracking of people in motion, without their knowledge and over a period that can be of long duration. Moreover, more than the cameras currently in use, these surveillance devices are likely to affect the exercise by citizens of other fundamental freedoms (including their right to demonstrate, freedom of worship, freedom of expression). The **CNIL** therefore considers that it would be preferable for the lawmaker to make the use of airborne cameras conditional on prior experimentation. The **CNIL** recalls that the framework to be developed for the use of new video devices, in particular drones, must ensure that, once their necessity has been proven, the infringements likely to be made on privacy are strictly proportionate to the purposes pursued. In this context, the **CNIL** considers it essential to : – further limit the purposes for which these devices may be used	Date of CNIL's opinion: 11 January 2021 Date of CNIL's statement: 3 February 2021	CNIL's opinion (in French) Link CNIL's statement (in French) Link

Development	Summary	Date	Links
	– ensure that the specific circumstances of the missions carried out justify their use, for a period of time appropriate to these circumstances – strengthen the guarantees surrounding their implementation Other observations were also made by the **CNIL** on the provisions of the draft law concerning individual cameras, cameras in certain vehicles, and video protection, in particular on the real-time transmission of images to law enforcement agencies. In general, the **CNIL** stresses that the normative framework as envisaged, and the resulting developments, still do not, in its view, provide a legal framework that is sufficiently protective of individuals' rights.		
The CNIL imposes penalties on a data controller and its subcontractor for credential stuffing attacks	From June 2018 to January 2020, the **CNIL** received several notifications of personal data breaches related to a website from which several million customers regularly make purchases. During its investigations, the **CNIL** found that the website had suffered numerous waves of credential stuffing attacks. In this type of attack, a malicious person retrieves lists of "unencrypted" logins and passwords published on the internet, usually following a data breach. Assuming that users often use the same password and login for different services, the attacker will use "bots" to attempt a large number of logins to sites in order to access the information associated with the accounts. The **CNIL** found that attackers were able to obtain the following information: surname, first name, email address and date of birth of customers, as well as their loyalty card number and balance and information related to their orders. The **CNIL** found that the two companies had failed in their obligation to preserve the security of customers' personal data, as required by Article 32 GDPR. Indeed, the companies were late in putting in place measures to effectively combat these repeated attacks (i.e. a year from the first attacks). The **CNIL** imposed two separate penalties of EUR 150,000 for the controller and EUR 75,000 for the processor, in view of their respective responsibilities.	27 January 2021	CNIL's statement (in French) Link

Development	Summary	Date	Links
	The CNIL did not decide to make these decisions public. Nevertheless, it wishes to communicate on these decisions in order to alert professionals to the need to increase their vigilance regarding credential stuffing attacks and to develop, together with their processor, sufficient measures to guarantee the protection of personal data.		
The CNIL issues a support charter for professionals	Advising and supporting professionals is one of the **CNIL's** essential missions. To help them comply, it provides various tools (guidelines, recommendations, practical guides, models, practical sheets on its website, etc.). In order for professionals to have a clear vision of the scope and terms of this support, the CNIL has decided to publish a charter. Its objective is to present the main principles and methodology, and to provide the professionals concerned with answers to their practical questions on the scope of requests for advice and the confidentiality of their exchanges with the **CNIL**. The publication of this charter is part of the **CNIL's** overall strategy to ensure a balance between repressive action and support. It will be supplemented by the publication of an annual work programme on soft law tools, in order to give professionals full visibility and enable them to participate (e.g. public consultations).	12 February 2021	CNIL's charter (in French) Link CNIL's statement (in French) Link
The CNIL launches a GDPR "sandbox" to support innovative projects in the field of digital health	The **CNIL** wishes to supplement its traditional instruments for supporting innovation by setting up a "sandbox". It will provide enhanced support, for a set period of time, to the leaders of emblematic projects in terms of personal data protection. The sandbox is open to all innovative projects, regardless of their status (public or private), size, maturity (start-up or existing player), or sector (industry, services, etc.), but to be really useful, it does not target operational or already launched projects. In 2021, for its first year, the **CNIL's** sandbox is open to three innovative projects in the field of digital health. The call for projects was open until 2 April 2021.	15 February 2021	CNIL's statement (in French) Link

Development	Summary	Date	Links
The CNIL closes the formal notice against EDF for the use of LINKY smart electricity meters	On 11 February 2020, the **CNIL** issued a formal notice against EDF concerning their processing of electricity consumption data collected in connection with the LINKY smart electricity meters. Following a control, the **CNIL** had found that the consent of users for the collection of their half-hourly consumption data was neither specific nor sufficiently informed. In addition, it appeared that EDF kept this data for an excessive period of time in relation to the purposes for which it was processed. The **CNIL** decided to give the company formal notice to comply with the GDPR within three months, which was extended due to the health crisis linked to COVID-19. The response provided by the company showed that the shortcomings observed during the inspection have since ceased, in particular due to the implementation of: – a new consent procedure – a new retention policy for consumer data The **CNIL** therefore decided on 15 February 2021 to close the formal notice.	16 February 2021	
The CNIL issues a referential of criteria for the certification of data protection training providers	Certification based on the **CNIL** referential allows training providers to obtain a seal of recognition certifying the quality of the training they provide in this field. A training course provided by a certified training provider can be based on the guarantees provided by compliance with the criteria of the referential, namely: – a base of skills and competences defined by the **CNIL** – content that is regularly updated to take into account current developments in data protection – speakers involved according to their skills and their ability to meet the specific objectives of each training course (e.g. a particular sector of activity, topic or personal data processing) Certification is not compulsory to offer data protection training. It is a voluntary mechanism allowing training organisations to	17 February 2021	CNIL's referential (in French) Link CNIL's statement Link

Development	Summary	Date	Links
	justify that their service is in line with the GDPR and the French Data Protection Act. In addition, higher education institutions benefit from other recognition systems. The publication of the certification criteria is the first step in launching the certification of data protection training providers. Thus, training providers who wish to obtain certification as soon as possible have a period of about 10 months to comply with the criteria and prepare their application. At the end of this preparatory period, training providers may apply for certification with one of the approved certification bodies listed on the **CNIL** website. The referential includes nearly thirty criteria aimed at demonstrating the qualification of the training provider in data protection. These requirements are divided into the following themes: – general requirements – information to the public on the training offered – identification of training needs and objectives – design of training courses – preparation and adaptation of training courses to learners – the conditions for carrying out the training – the skills of the trainers – the collection of assessments and the consideration of complaints		
The CNIL issues a warning to a sports club willing to use a facial recognition system	Following reports of a sports club's implementation of a facial recognition system for spectators, the **CNIL** decided to carry out controls on the use of this technology. This system, which was in the experimental phase, was intended to identify persons subject to a commercial stadium ban, to detect abandoned objects, and to fight terrorism. Analysis of the characteristics of the planned system showed that it was based on the processing of biometric data, whose collection and processing is prohibited by the GDPR and the French Data Protection Act, unless certain conditions are met. Moreover, in the	18 February 2021	CNIL's statement (in French) Link

Development	Summary	Date	Links
	absence of a special legislative or regulatory provision, the implementation of such a system by a sports club for "anti-terrorist" purposes is illegal. The **CNIL** therefore warned the sports club that, in the current legal framework, the envisaged processing could not be implemented in a lawful manner.		
The CNIL issues guidance on respecting people's rights when using chatbots	Chatbots allow a user to chat with a program designed to provide information. Personal data is often processed in the context of their use. Thus, in addition to the main principles that must be taken into account for any processing of personal data, the **CNIL** emphasises that the data controller or the processor implementing a chatbot must pay particular attention to the issues at stake for the rights and freedoms of individuals. Concerning data retention, in order to ensure the technical continuity of the chatbot or to keep a history of the conversation between the different pages of the site where it is present, a cookie is frequently placed and read on the user's terminal. Such an action is governed by Article 82 of the French Data Protection Act, on which the **CNIL** has published guidelines and recommendations. There are two possibilities for the chatbot operator: – either the operator wishes to be able to deposit a cookie prior to the activation of the chatbot. In this case, he must obtain the user's prior consent, which must be free, specific, informed and unambiguous – the cookie is only deposited when the user activates the chatbot (for example, by clicking on the conversation window displayed beforehand). It is then "strictly necessary for the provision of an online communication service at the express request of the user" and therefore does not require the user's consent. This exemption can only be used if the tracker is only used to provide the chatbot; any other purpose attached to it will require the user's consent Furthermore, the **CNIL** recalls that a conversation with a chatbot without human intervention cannot lead to important decisions for the data subject, such as the refusal of an online credit application, the application of higher rates or applying for a job.	19 February 2021	CNIL's statement (in French) Link

Development	Summary	Date	Links
	On the other hand, this conversation may be part of a wider process that would include significant human intervention. Indeed, automated decision making, where it has legal consequences or significantly affects a person in a similar way, is prohibited by Article 22 GDPR, unless measures have been implemented to safeguard the rights, freedoms and interests of the data subject and apart from the several exceptions (i.e. explicit consent, the decision is necessary for the performance of a contract, the decision is authorised by EU/Member State law). Finally, as for the management of notepad and comment areas, special attention must be paid to sensitive data. Such data can be processed in two situations. – If the collection is foreseeable and the processing is relevant (for example, with the chatbot of a health-related assistance service). It must then be ensured that the data processing falls within one of the exceptions set out in Article 9.2 of the GDPR. The processing of sensitive data is one of the nine criteria that may lead to a data protection impact assessment (DPIA). – If the collection is not predictable: sensitive data may be directly provided by the user. In this case, organisations are not required to obtain prior consent. However, they must implement mechanisms to minimise the risks to the rights and freedoms of individuals such as: – communicating, before any use of the chatbot, a warning inviting people to refrain from communicating sensitive data – implementing a purging system, either immediately or at least regularly, as the retention of this sensitive data is not relevant		
The CNIL closes the formal notice against the Ministry of the Interior concerning the automatic reading of number plates by speed cameras	On 4 December 2019, the **CNIL** issued a formal notice to the Ministry of the Interior concerning the automatic reading of vehicle number plates by speed cameras managed by the Ministry. Following controls, the **CNIL** found that the speed cameras retained the number plates of vehicles that had not committed an	Date of CNIL's decision: 19 February 2021 Date of CNIL's statement: 30 March 2021	CNIL's decision (in French) Link CNIL's statement (in French)

Development	Summary	Date	Links
	offence for a period that was excessive in relation to the purpose of the processing. The controls also established the inadequacy of the security measures concerning the processing: the passwords for the accounts allowing access to the speed cameras were not robust enough, the traceability of access was imperfect and the management of access rights to the application at the level of the Ministry's service provider was insufficient. The **CNIL** ordered the Ministry of the Interior to comply with the GDPR within three months, which was extended due to the health crisis linked to COVID-19. The answers provided by the Ministry showed that the breaches observed during the control had ceased, in particular due to: – the implementation of a computerised system that automates the destruction of personal data stored in the radar scanners beyond 24 hours – the reinforcement of security measures for speed cameras by implementing better rights management and a new policy on passwords for connecting to the speed cameras. The **CNIL** therefore decided, on 25 March 2021, to close the formal notice.		Link

Germany

Contributors

Alexander Niethammer
Managing Partner Germany
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

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

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

Philip Kuehn
Associate
T: +49 40 80 80 94 413
philipkuehn@
eversheds-sutherland.com

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

Development	Summary	Date	Links
No GDPR damages without proof of damage	In its ruling of February 25, 2021, the Regional Labour Court of Stuttgart decided that the granting of damages under Art. 82 GDPR always requires concrete evidence of the damage suffered by the data subject. A violation of data protection regulations itself is regularly not sufficient for this. Rather, it is precisely the violation of the law that must cause damage or the violation of the law must at least be one of the causes of the damage. An unrestrained expansion of the claim for damages is contrary to the principles of German and European law.	25 February 2021	Decision Link
The amount in dispute for a request for information is more than EUR 5,000	The German courts are very inconsistent with regard to the amount in dispute for requests for information under Art. 15 GDPR. While the Nuremberg Higher Labour Court (LAG) has set the amount in dispute at only EUR 500, the Cologne Higher Regional Court (OLG) partly assumes an amount in dispute of EUR 5,000. The Cologne Regional Court (AG Köln) has now	1 January 2021	Decision Link

Development	Summary	Date	Links
	followed this opinion and denied jurisdiction based on a value in dispute of EUR 5,000.		
Use of Mailchimp only permissible after balance of interests	The Bavarian State Office for Data Protection Supervision prohibited a Munich-based company from using the email provider Mailchimp. The reason for this was that since the Schrems II ruling of the European Court of Justice, certain requirements must be met for a data transfer to the US. The company, on the other hand, used Mailchimp without a deeper examination of the legitimate interests. Consequently, it is not the use of Mailchimp itself that is prohibited, but rather the company must first weigh up the interests and ensure an appropriate level of data protection when transferring data to the US.	24 March 2021	Article Link
Controllers must always respond to requests for information, even if no data are available	The Lehrte District Court ruled that data controllers must always provide negative information when a GDPR right to information is enforced. This is obligatory even if no data is available at all. Simply not answering the request in such cases is not justified.	3 February 2021	Decision Link
300,000 EUR fine against football club VfB Stuttgart for unauthorised data transfer	The State Data Protection Commissioner of Baden-Württemberg imposed a fine of EUR 300,000 on the football club VfB Stuttgart. The reason for this was that the club had not ensured the required contractual provisions on data transfer when cooperating with an external service provider and had also violated data protection documentation obligations. The amount of the fine took into account that the club had cooperated extensively and implemented the requirements immediately.	10 March 2021	Press Statement Link
No admissibility of telemarketing in case of email opt-in	The Higher Administrative Court of Saarland ruled that an opt-in of a data subject, which is obtained in the context of an online competition by means of a DOI procedure via email cannot constitute a legal basis for marketing measures by telephone. This is because it is technically not possible to clearly ensure that the owner of the respective email address is also the owner of the respective telephone number entered. In such situations recourse to the legitimate interests of the data controller is also usually not sufficient.	16 February 2021	Decision Link

Germany

Development	Summary	Date	Links
Obligation to submit to the European Court of Justice in case of rejection of a GDPR claim for damages for failure to meet the materiality threshold	In its decision of 14 January 2021, the Federal Constitutional Court ruled that if a German court rejects a claim for damages under Art. 82 GDPR on the grounds that the threshold of materiality has not yet been reached, it must refer this question to the European Court of Justice. This is an unresolved legal issue, as the materiality threshold of Art. 82 GDPR requires a broad interpretation and the **ECJ** must define the criteria for this more precisely.	14 January 2021	Decision Link
Transport encryption for emails generally sufficient as a GDPR security measure	The Administrative Court of Mainz ruled that transport encryption of emails is regularly sufficient to assume an adequate level of data protection according to Art. 32 GDPR. This also applies in principle to professional secrecy holders such as lawyers, tax advisors or notaries. In deviation from this principle, content encryption is to be required if special indications justify an increased need for protection.	1 January 2021	Decision Link
Burden of proof when claiming GDPR damages lies with the plaintiff	The Frankfurt am Main Regional Court ruled that the data subject claiming damages under Art. 82 GDPR carries the full burden of proof regarding a data breach. For example, it must be proven that a specific data leak led to advertising calls. It is not sufficient, however, if there were only data leaks at the company in the past, which led to such advertising calls.	18 January 2021	Decision Link
Hamburg data protection commissioner requests for information against Clubhouse app	The Hamburg data protection commissioner has launched an official request for information against the US provider of the app Clubhouse. The app raises many questions about the privacy of users and third parties. In particular, the reading of the app's address books, the recording of conversations and the lack of transparency in Clubhouse's data processing are controversial.	2 February 2021	Press Statement Link
Competence of the national data protection authorities in cross-border cases	In his opinion on the competence of national data protection authorities in cross-border cases, the Advocate General of the European Court of Justice stated that in principle the data protection authority of the State, where the head office of the data controller is located, has the general competence to initiate judicial proceedings for GDPR violations. Despite that, the national data protection authorities in whose territory the controller operates are entitled by the GDPR to initiate	13 January 2021	Press Statement Link

Development	Summary	Date	Links
	proceedings in their respective member states. The leading data protection authority also has to cooperate closely with all other data protection authorities.		
Fine of EUR 10.4 million against notebooksbilliger.de for inadmissible video surveillance	The State Commissioner for Data Protection of Lower Saxony imposed a fine of 10.4 million euros on notebooksbilliger.de AG on the basis of Article 83 GDPR. The reason for the fine was a data protection violation against the data protection rights of employees, as the company monitored its employees by video over a period of at least two years and in many cases stored these recordings for 60 days without having a legal basis for doing so. The cameras included workplaces, sales rooms, warehouses and common areas, which also recorded customers. The company justified this procedure by stating that the aim of the installed video cameras was to prevent and solve criminal offences and to track the flow of goods in the warehouses. However, in order to prevent theft, a company must first consider milder means (e.g. random bag checks when leaving the premises), as video surveillance represents a particularly intensive intervention in the right of personality, because it can theoretically be used to observe and analyse a person's entire behaviour. Moreover, video surveillance for the detection of criminal offences is only lawful if there is reasonable suspicion against specific individuals, whereas general suspicion is again not sufficient. In the case of reasonable suspicion against individual persons, however, surveillance must be limited in time. None of these criteria were met in this case. Notebooksbilliger.de cooperated with the data protection authority and has since made the video surveillance lawful. The company is challenging the decision, arguing that the amount of the fine is excessive and that the company's behaviour is standard market practice for mail order and logistics service providers.	8 January 2021	Press Statement Link

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

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

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

Jamie Leung
Trainee Solicitor
T: +852 2186 4987
jamieleung@
eversheds-sutherland.com

Development	Summary	Date	Links
Hong Kong Government proposes amendments to the Personal Data (Privacy) Ordinance (Chapter 486, Laws of Hong Kong) ("PDPO") to combat doxxing	To combat doxxing (which is generally the act of publicly revealing previously private personal information about an individual or organization), the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") has been actively working with the Hong Kong Government in formulating concrete proposals to amend the **PDPO**, particularly in areas such as the definition of the offence of doxxing, penalties, evidential threshold, and the **PCPD's** statutory criminal investigation and prosecution powers. The **PCPD** will make reference to relevant laws in other jurisdictions as appropriate.	4 February 2021	PCPD Media Statement Link
PCPD assures the public that the "LeaveHomeSafe" Mobile App ("LeaveHomeSafe") is in	To alleviate public concerns over the protection of personal data privacy relating to the use of LeaveHomeSafe, a contact tracing mobile app launched by the Hong Kong Government in an attempt to curb the spread of COVID-19, the PCPD considered	19 February 2021	PCPD Media Statement Link

Development	Summary	Date	Links
compliance with requirements of privacy law	LeaveHomeSafe to be in compliance with the **PDPO** due to the following observations: – LeaveHomeSafe does not have a location tracking function. Neither does it collect users' GPS data. Therefore LeaveHomeSafe does not have the function of tracking users' movements. – The downloading of LeaveHomeSafe, which can be used immediately after download, does not involve registration of the users' personal data. No collection of any personal data is involved during the process of download. – Visit records are kept on users' mobile phones only, not in any government system. There is no transfer of personal data to the government system or operators of premises for retention. Only in the event of a confirmed infection will the infected person be required by law to upload the relevant visit records and provide his/her name and contact information to assist the health authorities in contact tracing. – Visit records will be automatically erased after 31 days.		
PCPD submits response to the consultation paper on real-name registration for SIM cards	On 30 January 2021, the Commerce and Economic Development Bureau ("**CEDB**") launched a public consultation on the proposal to implement a real-name registration programme for SIM cards through a regulation made pursuant to the Telecommunications Ordinance (Chapter 106, Laws of Hong Kong) ("**TO**"). Should the proposal be implemented, the regulation will provide the necessary legal basis for telecommunications operators to register, collate and retain the registration information of users as required. The proposal seeks to plug the loophole caused by the anonymous nature of SIM cards, especially pre-paid SIM ("**PPS**") cards, and to facilitate the prevention and detection of crimes related to the use of PPS cards. In its written submission to the **CEDB** dated 17 March 2021, the **PCPD** made the following reminders and recommendations: – Mobile service operators will have to comply with the requirements of the **PDPO**, including the data protection principles stipulated therein, as regards the collection,	17 March 2021	Government press release dated 29 January 2021 Link Consultation paper dated 30 January 2021 Link PCPD news dated 17 March 2021 Link PCPD written submission dated 17 March 2021 Link

Development	Summary	Date	Links
	holding, processing and use of personal data provided by SIM card subscribers. – Personal data should only be collected if it is collected for a lawful purpose and necessary for or directly related to the purpose(s) of the proposed programme, and is adequate but not excessive in relation to such purpose(s). – Instead of requiring every subscriber to provide a copy of the identity document for registration, subject to operational feasibilities, subscribers should be given the following options: – They may choose to register online, and in such a case they would have to provide a copy of the identity document for verification purpose; or – They may choose to register in person at the service operators' offices or shops, and in such a case they would only have to produce the original identity document for verification by the staff, but do not have to provide a copy for retention. – Subscribers' personal data shall not be kept for a period longer than is necessary for the fulfilment of the purpose(s) for which the data is to be used. A definite duration (say, not more than 12 months) should be prescribed. – The circumstances under which law enforcement agencies could request service operators to provide subscribers' registration records should be clearly spelt out in the legislation. – The Communications Authority in its guidelines to service operators should set out in detail the technical security measures to be taken, and the Communications Authority should regularly carry out inspections of the systems/database used by the service operators to ensure that adequate data security measures have been put in place. – Service operators should take all practicable steps to ensure openness and transparency of their personal data policies and practices.		

Development	Summary	Date	Links
	– With a view to providing sufficient deterrent effect, the Communications Authority could make use of its power under the **TO** to impose financial penalties on service operators who fail to observe the relevant requirements under the proposed programme. The consultation period ended on 20 March 2021. As of the date of this edition of Updata, the consultation report has yet to be published.		

Hungary

Contributors

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

Ádám Takács
Paralegal
T: +36 1 39 43 12 1
takacs@
eversheds-sutherland.hu

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

Development	Summary	Date	Links
Recommendation of NADP on Certain Data Protection Requirements related to the Data Processing of Political Parties and Organizations	The Authority complements its previous recommendation as it considers it necessary to highlight the additional data protection requirements that will be addressed in the future with regard to the data processing of political parties and organizations. Data processing operations carried out by political parties and organizations typically occur in the following activities: – collecting a sufficient number of recommendations for the announcement of candidates and lists – building a sympathy database – delivery of campaign materials to voters – signature collections organized to achieve a political goal – political marketing activities In the next election period, the Authority will hold the persons and organizations involved in the data processing of political organizations accountable to account for compliance with the requirements related to the responsibility of data controllers as follows: – Prior to the commencement of data processing operations, these organizations shall clearly define the role of the party,	17 March 2021	Link

Development	Summary	Date	Links
	political organization or member, activist or candidate in the data processing activities. – Political organizations should not collect or record special categories of personal data other than those strictly necessary for the purpose of data processing during the collection of recommendations / signatures. – Personal data must be suitable for the purpose for which they are processed and relevant to the purpose, and the scope of the data must be limited to the minimum necessary for that purpose. – Greater attention needs to be paid to ensuring the accuracy of the data, especially for data from different sources. During the collection of signatures, it is unnecessary and disproportionate to request any identity document to prove the identity of the signatory of the questionnaire / recommendation form. – Political parties and organizations need to develop appropriate internal procedures to ensure the rights of the data subjects. In order to be able to exercise the rights of the data subject, appropriate information on the course of the exercise of rights and contact details must be provided. – Political parties should make their data processing transparent, clearly present their data processing activities, and make data processes of the personal data transparent. They should also develop data processing information sheets for all their data process and publish them in an easily accessible way. – In the case of a telephone call or e-mail for political marketing purposes connected with a poll organized for political purposes, simple, comprehensible information on the circumstances of data processing must be provided, including basic information on the interface where the data is available.		
Court of appeal decision regarding camera systems operated by condominiums	In this case, the court of appeal found that where camera systems are operated by condominiums, the condominium can generally be considered a data controller and the service provider operating the camera system as a data processor or data	17 March 2021	Link

Development	Summary	Date	Links
	controller, depending on the circumstances of the case. In the specific case, the service provider operating the camera system was also considered a data controller. The court of appeal was able to decide on the question of whether the data processing was lawful for the service provider after determining that it was a data controller. In its judgment, the court of appeal found that a breach of data processing rules did not in itself amount to an infringement of the right to the protection of personal data. The court of appeal argued that the defendant was right to claim that on the office door there was a pictogram indicating the installation and use of the camera. However, the plaintiff's conduct by entering into the office does not constitute consent to the processing of his personal data. Consent is considered to have been given only if it has been preceded by complete information containing the purpose and method of data processing. The pictogram on its own does not meet this requirement. In its judgment, the court of appeal found that the defendant had acted unlawfully in processing the plaintiff's personal data. Subsequently, the court of appeal assessed that the defendant had used the personal data that had been handled in an infringing manner, had not deleted it at the request of the plaintiff, and still retained it. This also meant a violation of the plaintiff's right to self-determination stemming from human dignity, including his right to his image as personal data.		
Hungarian DPA Guidance for employers' if they can request employees to share whether they are protected against COVID-19	The DPA has received several inquiries from employers as to whether they are entitled to process data on the fact that employees are immune fromt COVID-19.. The DPA emphasizes the fact that protection, i.e. either recovery from the disease or vaccination, constitutes health data. According to the **DPA**, for the purposes of labor law, occupational safety, occupational health and work organization, on the basis of a risk analysis, it may be necessary and proportionate for the employer to know the employee's protection against the coronavirus in certain occupations or among employees.	17 March 2021	Link

Development	Summary	Date	Links
	The knowledge of protection status by the employer may be necessary and proportionate to protect the life and health of the protected employee, other employees and third parties potentially coming into contact with the employee, and to comply with the employer's obligations in this regard. The **DPA** also highlights that the purpose of such data processing should be that the employer takes the necessary measures to comply with labor law rules. This purpose must be actual and real. Data processing must be designed with compliance with the principle of accountability. Nor should the principle of data protection, which stipulates that only data that is strictly necessary and proportionate to achieve the purpose may be processed, be disregarded. Regarding necessity, the **DPA** reiterates that the employer must carry out the assessment per job or per employee. An application or a protection certificate, can serve to prove as protection against the coronavirus.		

Ireland

Contributors

Marie McGinley
Partner & Head of Intellectual Property, Technology & Data Protection

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

Development	Summary	Date	Links
Eversheds Sutherland article on EU-UK data transfers post Brexit	This article reviews the grace period in respect of data transfers between the EU and the UK. The Withdrawal Agreement provides that personal data can flow freely from the EU to the UK (without the need for additional measures) from the 31 December 2020 for (i) a period of four months (which can be extended for a further two months if neither party objects), or (ii) on the date the UK is provided with an Adequacy Decision (under Article 45 of the GDPR), whichever is the earlier. Please be aware that there will be further updates on this topic, as the position is under review.	11 January 2021	Eversheds Sutherland article Link
DPC publishes guidance on the use of domestic CCTV	This DPC guidance discusses the use of domestic CCTV and the CCTV complaints that the **DPC** can handle. The guidance provides that the **DPC** is in receipt of a large number of complaints from individuals about the operation of CCTV in a domestic setting, usually at neighbouring properties. In some cases, the complaints to the **DPC** relate to a broader dispute between neighbours and in such circumstances the **DPC** can address only the personal data processing issues that arise.	14 January 2021	DPC Guidance Link
Eversheds Sutherland article on the EU Cyber Strategy	This article discusses the new EU Cybersecurity Strategy (the "**Strategy**"), which the EU Commission published in December 2020, to enhance "collective resilience against cyber threats and ensure citizens and businesses across the EU can fully benefit from trustworthy and reliable services and digital tools".	4 February 2021	Eversheds Sutherland article Link

Ireland

Development	Summary	Date	Links
Eversheds Sutherland article – Telescope – TMT Outlook 2021	This article sets out what will impact the technology, media and telecom ("**TMT**") sector in 2021.	9 February 2021	Eversheds Sutherland article Link
DPC issues guidance on CCTV, discovery and access requests	In a decision of the High Court in November 2020 (Dudgeon v Supermacs Ireland Ltd., [2020] IEHC 600), the court ruled that a restaurant was not obliged to disclose CCTV recordings of an incident to a person identifiable on the recording and who claimed damages for injuries resulting from that incident. The DPC provides that the court's decision in this case is focussed on the law concerning discovery and is not in reference to or related to data protection rights.	10 February 2021	DPC Guidance Link
Eversheds Sutherland article on data centres – how District Heating Schemes can contribute to solving the climate change crisis with help from data centres	This article focuses on District Heating, its role in de-carbonising Ireland and how data centres can contribute to this.	10 February 2021	Eversheds Sutherland article Link
Eversheds Sutherland article on the ePrivacy Regulation	This article highlights how the ePrivacy Regulation will update existing rules on the protection of privacy and confidentiality in the use of electronic communication services.	18 February 2021	Eversheds Sutherland article Link
DPC publishes 2020 annual report	The annual report provides an insight into the work of the **DPC** during 2020, key areas of interest the **DPC** has identified and information on the number of data breaches, complaints, enquiries etc received by the **DPC** during this time.	25 February 2021	DPC Guidance Link DPC annual report Link
DPC provides insight into correspondence with the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament ("LIBE committee")	The **DPC** contacted the LIBE Committee in February and March 2021 on foot of the publication of two draft resolutions and connected amendments proposed for adoption by that Committee. The **DPC** provides that these resolutions and proposed amendments were published in circumstances where the Committee directed significant criticism exclusively at the Irish	17 March 2021	DPC Guidance Link

Development	Summary	Date	Links
	DPC and where the Committee's information was both inaccurate and incomplete. The **DPC** has now published the full suite of the correspondence between the **DPC** and the Committee both as a means to facilitate responding to a significant volume of media queries to the office and in order to provide context in terms of the media reports already published.		
DPC issues guidance on the 'Children's Fundamentals' and how to protect children's personal data	The DPC published a comprehensive draft guidance document at the end of last year entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (or "**the Fundamentals**" for short). **The Fundamentals** set out 14 key principles for organisations to follow when processing children's data, and should be complied with by all organisations processing children's data. This includes services that are directed at / intended for, or are likely to be accessed by children. In Ireland, for data protection purposes, a child is somebody under the age of 18 years.	18 March 2021	DPC Guidance Link
DPC launches inquiry into the processing of personal data by the Department of Health	The **DPC** has launched a statutory inquiry under Section 110 of the Data Protection Act, 2018 arising from revelations concerning the processing by the Department of Health of the personal data of children with autism who were involved in legal actions against the State. The inquiry will examine whether or not the Department of Health has discharged its obligations in connection with the data processing concerned and it will determine whether or not any provisions of the Data Protection Acts and/or the GDPR have been contravened by the Department of Health in that context. A team of Authorised Officers has been appointed by the Commission to conduct the inquiry.	30 March 2021	DPC Guidance Link

Italy

Contributors

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

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

Development	Summary	Date	Links
IDPA approved a code of conduct on the use of health data for educational and scientific publication purposes	**IDPA** approved a code of conduct under Art. 40 GDPR on the use of health data that is already present in medical files of public health entities for educational and scientific publication purposes. The code was proposed by the Italian region of Veneto and by a local health institution (AULSS 9 Scaligera). This code provides, inter alia, for accountability measures, retention periods of the data taken into account, for technical annexes on anonymisation and pseudonymisation, for templates of request forms and information notices for data subjects.	14 January 2021	IDPA's measure approving the code of conduct (only available in Italian language) Link
IDPA issued an emergency measure against a social network imposing an immediate restriction to the processing of data of users whose age could not be established with certainty	**IDPA** imposed an immediate restriction to the processing performed by a social network with regard to the data of users whose age could not be established with certainty. On 22 January 2021, **IDPA** decided to take urgent measures following the dismay caused by the death of a 10-year girl. Previously **IDPA** had already notified several infringements to the social network, challenging, inter alia, the poor attention to the protection of minors, the easy dodging of the registration ban applied by the social network to children under 13 years, non-transparent and unclear information provided to users, and default settings falling short of privacy requirements. Pending receipt of the feedback that was requested, **IDPA** decided in any event issue a measure for the immediate protection to the minors in Italy that have joined the social network and banned the social network from further processing the data relating to any user 'whose age could not be established	Date of press release: 14 January 2021 Date of measure: 22 January 2021	IDPA's press release Link IDPA's measure Link

Development	Summary	Date	Links
	with full certainty so as to ensure compliance with the age-related requirements'. **IDPA** also brought this issue to the attention of the Irish Supervisory Authority, since the concerned social network communicated that it had set its main EU establishment in Ireland.		
IDPA's follow-up to the measure of 22 January on the restrictions imposed on a social network	On 14 January 2021, **IDPA** issued a press release declaring that the social network communicated its intention to implement measures to ban access to users aged below 13 years, to consider deploying AI-based systems for age verification purposes and to launch an information campaign to raise parents' and children's awareness. **IDPA** declared its intention to monitor the effectiveness of the measures to be enforced. The social network declared to **IDPA** its intention to: – block access by all Italian users as of 9 February 2021 and to request the date of birth to be re-entered in order to continue using its app. If an user's age is determined to be below 13 years, that user's account will be removed. In order to identify users below 13 years with reasonable certainty following this initial check, the social network undertook to further consider the deployment of AI-based systems and also implemented new functions in its app; – provide more information to users, also by launching information campaigns and sending alerts; – review and amend its privacy notice for users under 18 years of age. **IDPA** also declared its intention to launch an awareness-raising campaign jointly with a child protection charity. On 11 February, **IDPA** issued another measure, taking into account the declarations of the social network and extending the restrictions issued on 22 January until 15 March.	Date of press release: 14 January 2021 Date of measure: 11 February 2021	IDPA's press release Link IDPA's measure (only available in Italian language) Link

Development	Summary	Date	Links
IDPA updated its FAQs relating to Covid-19 and data protection relating to the vaccination of employees	On 17 February 2021, **IDPA** updated its FAQs relating to Covid-19 and data protection regarding the vaccination of employees. **IDPA** stated that the employer: – cannot ask its employees to provide information on their vaccination condition or a copy of documents demonstrating that they have been vaccinated against Covid-19 since this is not allowed by emergency and health and safety laws. The employer cannot deem lawful the processing of data relating to the vaccination on the basis of employees' consent, due to the fact that such consent cannot be a valid legal basis due to the imbalance between controller and data subject in the employment context – cannot ask the competent doctor to communicate the names of vaccinated employees. Only the competent doctor can process medical data of employees and, among such data, information relating to vaccination if applicable, in the context of the medical emergency and when assessing the suitability to the specific task. The employer can only acquire, relying on the laws currently in force, the suitability assessments to the specific task and possible prescriptions and/or restrictions thereby reported. **IDPA** also stated that awaiting an intervention from the legislator to assess – in the current epidemiological situation and on the basis of scientific evidence – if requiring anti-Covid-19 vaccination to perform certain professions, jobs and tasks, currently, in the cases of direct exposure to "biological agents" at work (as, e.g. in the healthcare context, implying higher risks to workers and patients), "special protection measures provided for some employment contexts apply under the Italian Health and Safety Law." In such a framework, only the competent doctor, due to his role to link the national/regional healthcare system with the specific employment context, in compliance with public health authorities' indications on the effectiveness and reliability of the vaccine, can process personal data relating to the vaccination of employees and, if applicable, take this into account in the assessment of their suitability to the specific task.	17 February 2021	IDPA's FAQs Link

Development	Summary	Date	Links
	The employer can only implement the measures indicated by the competent doctor in the cases of partial or temporary non-suitability of the employee to his/her specific task. A vaccination obligation was introduced by Law Decree n. 44 of 1 April 2021 for healthcare professionals and operators of healthcare interests.		
IDPA's public contest to identify solutions to make privacy information notices clearer and easier to understand.	IDPA launched a public contest to identify solutions to make privacy information notices clearer and easier to understand. Some potential methods for doing this would be icons, symbols or other graphic solutions. The contest is open to private undertakings, professionals and to anybody else who is interested. **IDPA** asks to send a set of symbols of icons able to fully represent requirements under articles 13-14 GDPR The deadline to send proposals is 30 May 2021. The solution chosen by **IDPA** will be made available by **IDPA** on its website.	15 March 2021	IDPA's press release (only available in Italian language) Link

Lithuania

Contributors

Rimtis Puisys
Partner
T: +37 0 52 39 23 73
rimtis.puisys@
eversheds-sutherland.it

Development	Summary	Date	Links
The State Data Protection Inspectorate sets out inspection schedule for 2021	The State Data Protection Inspectorate ("**SDPI**") scheduled inspections for 15 organisations. It plans to check several banks, credit unions and other organisations for the scope of personal data in the provision of payment initiation services. The processing of personal data in the context of financial services is a particularly sensitive area, as improper processing of personal data can lead to financial harm to the individual. Thus, the **SDPI**, when conducting inspections, will assess whether the organisations providing payment initiation services do not process excess personal data in order to ensure the rights of data subjects as much as possible.	9 February 2021	The list of planned inspections (in Lithuanian)
The State Data Protection Inspectorate initiates an investigation into the security of personal data of CityBee customers	In response to the information that appeared in the public sphere on 15 February 2021, that the CityBee customer database with personal data of individuals was stolen and leaked, the State Data Protection Inspectorate (**SDPI**), launched an investigation on its own initiative. It is publicly announced that data of about 110,000 customers was leaked. According to the legislation, the investigation carried out by the supervisory authority may last up to 4 months, with the possibility to extend it for a longer period, depending on the circumstances and course of the investigation. According to Raimondas Andrijauskas, Director of **SDPI**: "Currently, all the institutions involved in the incident are cooperating to prevent possible further illegal processing of personal data as much as possible, pay ransoms, and keep track of our and the police's information about the incident. "	16 February 2021	

Development	Summary	Date	Links
Summary of case law in the field of personal data protection of 2020	The State Data Protection Inspectorate ("**SDPI**") summarised court decisions examining cases concerning complaints of persons investigated by the SDPI. This summary provides details of 21 court decisions that took place prior to 31 December 2020. Of these, 10 were decisions of the Vilnius Regional Administrative Court, which were not appealed, and 11 decisions of the Supreme Administrative Court of Lithuania. In 15 cases the decisions of the **SDPI** were declared valid and upheld, in 4 cases the decisions of the **SDPI** were upheld in part and annulled in the other part, and in two cases the decisions of the **SDPI** were annulled and the complaint was re-examined.	2 March 2021	Link to the summary (in Lithuanian): Link
Legislation governing the certification mechanisms provided for in the GDPR is subject to public consultation	The State Data Protection Inspectorate ("**SDPI**") submitted for public consultations a draft order of the Director of **SDPI**, which approves: – Description of the procedure for accreditation of certification bodies (the requirements for accreditation of certification bodies are set out in the Annex to this Description) and – A description of the procedure for approving certification criteria developed by certification bodies. – The procedure set out in this draft order is important in determining the methodology for assessing certification bodies and their chosen certification tools, thus ensuring that controllers and / or processors seek to further substantiate their activities or individual personal data processing operations with GDPR requirements and increase trust in their services. Accreditation of certification bodies and their future certification is a voluntary measure that can be taken by data controllers and / or processors. Following the evaluation of the comments and suggestions received during the public consultation, the requirements for the accreditation of certification bodies in accordance with Article 64	19 March 2021	Link of the draft (in Lithuanian) Link

Development	Summary	Date	Links
	(1) (c) of the GDPR will be submitted to the European Data Protection Board for assessment.		

Malaysia

Contributors

Brian Law
Regional Head of IP
T: +65 6361 9873
brianlaw@
eversheds-harryelias.com

Suaran Singh Sidhu
Partner
T: +603 9212 9287
suaransidhu@
law-partnership.com

Development	Summary	Date	Links
Notice of Guidelines for the Purpose of Buying, Using and Processing a Cellular Booster or Repeater ("CBR").	The Malaysian Communications and Multimedia Commission ("**MCMC**") found an increase in cases of spectrum interference involving the use of non-compliant **CBR**. **CBR** is a mobile network device that adds signal strength from transmitting stations as well as mobile devices. The increase of irregular use of **CBR** tools by the public and service provider companies will likely cause a disruption to the quality of cellular networks and mobile broadband. To keep this issue under control, the **MCMC** issued guidelines on the purchase, use and ownership of Cellular Booster or Repeater ("**Guidelines**"), which came into effect on 1 January 2021. These Guidelines are intended to remind the public to obtain **CBR** equipment from legitimate cellular service provider companies and to refrain from buying any **CBR** equipment from unregistered sources. Failure to comply with these Guidelines is an offense under Section 239 of the Communications and Multimedia Act 1998 ("**CMA**") or Regulation 16 under the Communications and Multimedia (Technical Standards) Regulations 2000, which is punishable by a fine not exceeding RM500,000.00 or imprisonment not exceeding five (5) years or both at once.	9 January 2021	The Guidelines Link
Social Media Users Are Reminded to Maintain Politeness and Decency When Giving Views or Comments.	In light of the implementation of the second Movement Control Order ("**MCO**") to combat the spread of Covid-19 and the Proclamation of Emergency, the **MCMC** reminded the Malaysian public, especially social media users, of the importance of always maintaining decency when making comments and / or giving their views on social media.	12 January 2021	Press Release (Language: Malay – this press release was not translated into the English language)

Development	Summary	Date	Links
	In order to curb the spread of unauthentic information, obscene and inappropriate statements involving royalty, religion and race ("**3R**"), the **MCMC** will continue to monitor the same and will act upon complaints from the public in accordance with provisions of existing laws in a transparent manner. Any sharing of content that is false, obscene and threatening is an offence under Section 233 of the **CMA**. Conviction carries a maximum fine of RM50,000 or imprisonment for one year or both.		Link
Calling for Participation in Jalinan Digital Negara ("JENDELA") Phase 1 Initiative.	The **MCMC** issued a revised invitation ("**the Invitation**"), which replaces the previous invitation dated 20 November 2020, for interested and eligible licences registered under the **CMA** to participate in the installation of Network Facilities and deployment of Network Service for the provisioning of Public Cellular Services at the Universal Service Targets under the **JENDELA** Phase 1 initiative. The initiative aims to enhance nationwide coverage of 4G network in populated areas nationwide. The invitation encompasses a scope of work that is divided into two parts (either parts are optional to the interested and eligible licensees), which are: – Part 1: Covers the installation of passive infrastructure – Part 2: Covers the installation of active infrastructure and the deployment of public cellular services The closing date of registration was February 2021 and the submission of the Draft Universal Services Plans by the interested and eligible licensees was 31 March 2021.	15 January 2021	Press Release Link
"Beware of Scams Through Whatsapp Accounts", MCMC warns	There had been reports on frequents scams being carried out via Whatsapp. To combat this issue, the **MCMC** advised the public to be wary of fraudulent tactics aimed at taking over the users' Whatsapp accounts. Various tricks are carried out by the scammers to trick the users into submitting a 6-digit verification code received from Whatsapp. With this, scammers can take over the users' Whatsapp accounts. The verification code is generally received by the user for verification purposes when there is an attempt to exchange the phone number associated with a WhatsApp account.	21 January 2021	Press Release (Language: Malay – this press release was not translated into the English language) Link

Development	Summary	Date	Links
	MCMC detected several tricks often used by scammers, which are set out below: – Scammers impersonating as a friend or family member (by using the Whatsapp account of the friend / family which has been hacked by them) and subsequently appealed to the user for assistance to submit the received 6-digit verification code; – Scammers disguised themselves as Whatsapp employees and ask the user to submit the 6-digit verification code received – Scammers accidentally made several failed authentication attempts, which causes Whatsapp's system to make an automatic call to the user's number to inform them of the verification code. The scammer will either: – Communicate with the user, while in disguise, to obtain the verification code – If the user fails to answer the automatic call from Whatsapp and it goes to the user's mailbox, the scammer will attempt to guess the password or ask the user for the password to the user's mailbox to access the recording **MCMC** advised the public on some precautions to take to ensure they do not fall into the trap of these scammers, as set out below: – Be alert to requests for 6-digit Whatsapp verification codes from any parties – Never give the Whatsapp 6-digit verification code to any party – Never give their mailbox password to any party – Make sure the voicemail password is sufficiently complex.		
National Cyber Security Agency ("NACSA") issued a Warning Notice to All Government Agencies	**NACSA** issued a warning notice to all government agencies to prevent and minimise the impact of cyberattacks. This is pursuant to the spread of a video released in early January by a group of hacker activists known as "**Anonymous Malaysia**", which sent a warning message to the Malaysian Government leading to threats	27 January 2021	Official Article Link Link

Development	Summary	Date	Links
pursuant to hacker activists' threat.	of hacking official government websites. As posted on their social media account, "**Anonymous Malaysia**" stated that their warning should serve as a "wake up call to the Malaysian Government", which they have accused on keeping silent over the many data breaches and sales of personal information of citizens in the past few years.		
MCMC Continues to Increase Efforts to Address Internet Access Problems in Malaysia	The **MCMC** continues to enhance their efforts to address issues on Internet access faced by Malaysians nationwide. The **MCMC** went to review the situations at the complaint locations, some of which are set out below: – Selindang Village, Padang Tengku, Lipis – **MCMC** made a site visit to this village which has problems on poor internet coverage and connection. MCMC decided that a new communication tower will be built under the **JENDELA** plan which is expected to start in the third quarter of 2021. Meanwhile, the existing tower nearby will be upgraded to 4G coverage to improve the quality of broadband services in the village and several nearby villages. – Pos Brooke National School, Gua Musang – One of Malaysia's news portals, the Malay Mail, reported that Pos Brooke National School in Gua Musang has issues with accessing the Internet. Hence, **MCMC** decided that the communication tower near the Pos Brooke National School will be upgraded to 4G coverage under the **JENDELA** plan and it is expected to be completed by the end of 2021. This solution is expected to help more than 300 students of the said school. – Sungair Tengar Village in Tebuk Mufrad Sabak Bernam – There were reports by two Malaysia news portals, Sinar Harian and Berita Harian, on the issues of poor internet access faced by school students in the Sungai Air Tawar State Assembly. This caught **MCMC's** attention, in which **MCMC** visited the said location to check the quality of telecommunication network coverage of the area and get more information on the same.	18 February 2021	Press Release - 8 February 2021 Link Press Release - 18 February 2021 Link Press Release - 4 March 2021 (Language: Malay – these press releases above were not translated into the English language) Link

Development	Summary	Date	Links
	As a short-term solution, **MCMC** has contacted the telecommunication companies to implement the optimization of communication tower antennas in the village areas and is has been completed at the end of this February. For a long-term solution, a new tower will be built in the said area under the **JENDELA** plan, which is expected to begin at the end of 2021.		
MCMC's Oversight of Digital Nasional Berhad ("DNB") – The Malaysian's Government Special Purpose Vehicle for the Deployment of 5G.	The **MCMC** welcomed the announcement on the Special Purpose Vehicle by Malaysian's Ministry of Finance. **DNB**, which is the Special Purpose Vehicle announced to undertake the deployment of 5G infrastructure and network nationwide, will be licensed to operate under the **CMA**. Despite being an entity wholly owned by the Malaysian Government, **DNB** would be subject to **MCMC's** regulatory oversight, like any other licensee under the **CMA**. **MCMC** will regulate and monitor **DNB** via the relevant regulatory tools under the **CMA**. **DNB** will be the neutral party that enables other licensed telecommunication companies to focus on the latest technologies to develop innovative retail services as service offerings to consumers, enterprises and even the Malaysian Government. In overseeing **DNB**, **MCMC** will remain focused on ensuring improved quality and expanded coverage of digital connectivity, and to facilitate new economic growth for Malaysia through the opportunities that 5G will likely bring.	2 March 2021	Press Release Link

Netherlands

Contributors

Olaf van Haperen
Partner
T: + 31 1 02 48 80 58
olafvanhaperen@
eversheds-sutherland.com

Robbert Santifort
International Senior Associate
T: +31 10 2488 077
robbertSantifort@
eversheds-sutherland.com

Sarah Zadeh
International Associate I
T: + 31 1 02 48 82 66
sarahzadeh@
eversheds-sutherland.com

Frederique Swart
Legal Assistant
frederiqueswart@
eversheds-sutherland.com

Development	Summary	Date	Links
Booking.com fined for late reporting of data breach	The **DDPA** has imposed a fine of €475,000 on Booking.com for failure to report a data breach to the **DDPA** in a timely manner. During the data breach, personal data of more than 4,000 customers was stolen. By means of telephone calls, cyber criminals extracted login details for the accounts of employees of 40 hotels in the United Arab Emirates in a Booking.com system. The stolen personal data included customer's names, addresses, phone numbers and details about their booking. In the process, the cyber criminals also accessed the credit card details of 283 people. In 97 cases the security code of the credit card was also included. Booking.com was notified of the data breach on January 13, 2019, but did not report it to the **DDPA** until February 7 2019, which missed the requisite deadline by 22 days, as the data breach had to be reported to the **DDPA** within 72 hours. Affected customers were notified of the breach on February 4, 2019. In addition, the company took other measures to mitigate the damages, such as offering to reimburse any losses. Booking.com is not appealing or objecting to the **DDPA's** fine.	31 March 2021	DDPA Press Release Link

Netherlands

Development	Summary	Date	Links
DDPA receives 75 data breach notifications after leak in Microsoft Exchange Servers	On 19 March 2021, the **DDPA** published a press release regarding the 75 data breach notifications it had received from organisations who use Microsoft Exchange Server to receive and send email. According to the National Cyber Security Centre, at least 1200 Dutch servers have been affected by the data breaches. Through an existing vulnerability in the Microsoft software, cyber criminals were able to access email accounts, steal data and install their own software. The **DDPA** calls on organisations using Microsoft software to check their systems for cyber attacks and to stay alert for suspicious activity. The **DDPA** explicitly stated that organisations often fail to make timely notifications of data breaches. Currently, there are 9 pending investigations regarding data breaches that were not reported or not reported in time.	19 March 2021	DDPA Press Release Link
Court of Amsterdam ruled on the right of data portability and the right of access	This case is brought forward by a group of cab drivers ("**applicants**") employed by the company Ola Netherlands B.V. ("**Ola**"). The applicants make use of the "**Ola Driver App**" (digital platform of **Ola**), which is used to facilitate the linking of a passenger and a (cab) driver. The applicants have requested access to all personal data processed by Ola and to receive the personal data concerning them, in a CSV file, or by means of an API or a TTP. The Court of Amsterdam ruled that the request ordering the respondent to provide all personal data falling within the scope of Article 20 GDPR, is too general and unspecific to such an extent that is must be rejected. Article 20 GDPR does not impose an obligation to provide the personal data in a specific or by means of an API or a TTP. The format, including the personal data provided by the respondent, would not impair the data portability. Subsequently, the Court of Amsterdam ruled that, regarding the data subject access request, **Ola** should grant the applicants access to specific personal data in a specific format including: ratings given by passengers, fraud probability score, earning profile (form of profiling), irregularity reporting system data and the data that led to financial sanctions.	11 March 2021	Court Ruling Link

Development	Summary	Date	Links
The DDPA published the annual report on data breaches	In 2020, the **DDPA** received 23,976 data breach notifications. That is a decrease of 11% compared to 2019 and can be explained by the fact that collection agencies reported fewer data breaches. On the other hand, the number of reports in response to hacking, malware or phishing incidents has increased by 30% compared to 2019. In particular, larger organizations, which process personal data of many data subjects, seem to be targeted by such events. The **DDPA** is concerned about the continued rise in the number of reports following hacking, malware or phishing incidents. That is why the **DDPA** has chosen to devote extra attention to multi-factor authentication ("**MFA**") in this report. In 2020, the AP received at least 249 reports where **MFA** could have prevented the data breach from occurring. The **DDPA** estimates that by 2020 there will be at least 600,000 and at most 2,000,000 natural persons (potentially) involved in a (reported) data breach due to lack of **MFA**. It is important to note that in many cases, **MFA** is an essential and therefore mandatory measure to comply with the requirements of Article 5, paragraph 1 (f), Article 24 and Article 32 GDPR, and failure to apply **MFA** can lead to a violation of the GDPR. The **DDPA** will also monitor the use of **MFA** more strictly in the period to come. **DDPA's** recommendations regarding MFA include: – **MFA** is to be set for all systems where access control is set, and especially with external access control and systems that contain a lot of (sensitive or special) personal data. – Set **MFA** on (business) instant messaging services (such as Signal, Telegram and WhatsApp) and mail applications. – Continue to verify the effectiveness of access control. – From the internal oversight in the organization, identify which processing operations qualify for the use of **MFA**. The Netherlands is one of the top 3 European countries where most data breaches are reported. As the Netherlands is a highly digitised country, the risk of data breaches is relatively high. This also means that the Netherlands needs to pay extra attention to	1 March 2021	DDPA Report Link

Development	Summary	Date	Links
	fundamental issues such as privacy, the protection of personal data and cybersecurity. In addition to the 23,976 Dutch data breach notifications received by the **DDPA**, other European privacy regulators shared cross-border data breaches with the **DDPA** in 79 cases. Most data breach notifications in 2020 came from the health and welfare sector (30%), followed by financial services and public administration (both 22%). In 2020, the **DDPA** completed 10 investigations in cases where a notifiable data breach was not (or may not have been) reported. These investigations have resulted in either a warning letter or a disciplinary conversation. At the moment there are still 9 investigations pending.		
Amsterdam Court of Appeal ruled on removal of External Referral Register ("ERR") Registration	On 2 February 2021, the Amsterdam Court of Appeal ruled on a dispute concerning the deletion of personal data, regarding how the legal procedure in a preliminary relief proceedings relates to the special legal remedies in Article 35 Dutch GDPR Implementation Act ("**UAVG**"). The Court of Appeal reiterates that the legal remedy of Article 35 GDPR Implementation Act is the appropriate remedy. Not only is this ruling relevant for insurers and policyholders, but also for banks. The legal action of Article 35 **UAVG** provides an accessible way for the account holder to challenge decisions of the bank in court. An attorney is not necessarily required to initiate such legal proceedings. A request under Article 21 GDPR can be filed multiple times - and so can the procedure under Article 35 **UAVG**. The account holder who files a request at the bank after the six-week period has expired will have to prove the urgent interest in the relief sought even more. The account holder will have to demonstrate, and if necessary prove facts and circumstances from which the urgent interest can be derived. The mere statement that "by its nature the claim is urgent", as is sometimes assumed in lower courts, is not sufficient in this respect. Banks are regularly involved in preliminary relief proceedings, in which the requested remedy is to remove personal data, for example, to remove their registration from the External Referral	2 February 2021	Court Ruling Link

Development	Summary	Date	Links
	Register ("**ERR**") or from the register of the Dutch Credit Registration Agency ("**BKR**"). In cases in which the plaintiff has allowed the term of Article 35 (3) GDPR Implementation Act to expire, but has nevertheless commenced preliminary relief proceedings, the plaintiff will have to substantiate the urgent interest against the background of the system of Article 35 GDPR Implementation Act, subject to inadmissibility. This raises an additional threshold for the plaintiff, which banks can explicitly point out to judges - even though the court should assess this ex officio.		
Court of Breda ruled on whether competition is distorted by violation of privacy rules	On 3 February 2021, the District Court of Breda ruled on an interesting question in preliminary relief proceedings: is there distortion of competition when a competitor violates the privacy regulations? Two suppliers of GPS watches for the elderly believe that a competitor is able to supply cheaper watches in an 'unfair' way, by not adhering to the General Data Protection Regulation. Claimants Leading Care Technology ("**LCT**") and LifeWatcher filed preliminary relief proceedings against a third-party supplier of GPS watches, Avium. The defendant uses watches and software sourced from a Chinese company, which utilizes a server in Austria. According to the claimants, the defendant provides incorrect and incomplete information on its website regarding the use of the GPS watches, which would constitute unfair trade practices. It is also argued that the information in the defendant's privacy statement is incorrect and incomplete. By violating the rules in the field of consumer protection and privacy, the defendant would not only be acting unlawfully towards those involved, but also towards the claimants. The defendant can therefore supply the products cheaper, resulting in unfair competition and damage to its competitors, according to the claimants. The claimants base their claim on a wrongful act. They argue that the defendant is acting in violation of a legal duty and is allegedly violating the Dutch Unfair Trade Practices Act, the GDPR and the Dutch GDPR Implementation Act.	3 February 2021	Court Ruling Link

Development	Summary	Date	Links
	It is particularly interesting whether or not the standards of the GDPR also serve to protect the interests of competing companies. In this respect the Court in preliminary relief proceedings held that the GDPR does not contain any provision or consideration on the basis of which competitors can enforce the GDPR against each other. On the contrary, the Court explicitly referred to the Preamble to the Unfair Commercial Practices Directive and how this could have been invoked instead. The Court stated that the GDPR in fact grants this power (exclusively) to the data subjects themselves and to the **DDPA**. The fact that reliance by competitors on violations of the GDPR can lead to a strengthening of the protection of personal data, was insufficient reason for the Court to grant the claimants (as competitors) the right to enforce an injunction as claimed in court proceedings on the basis of the GDPR. In this case, the claimants have not sufficiently substantiated that there has actually been a violation of the GDPR and for that reason the claim cannot be granted.		
DDPA imposes fine on Dutch hospital for inadequate protection of medical records	The **DDPA** has imposed a fine of €440,000 on the Amsterdam-based hospital ("**OLVG**") for its inadequate protection of patients' medical records. Between 2018 and 2020 **OLVG** did not have sufficient safeguards in place to prevent unauthorized access to the records. It did not carry out proper checks of who had access to which records, and there were shortcomings in the information systems' security. In response to the **DDPA's** investigation, **OLVG** has made the required improvements. Patients have the right to expect that staff members will only access their medical records if it is necessary for the patient's treatment. **OLVG's** security measures couldn't guarantee that, which constituted a serious breach. Due to the severity of the breach, the **DDPA** has imposed this fine. Besides medical information, patient records also contain personal data like citizen service numbers, addresses and phone numbers. These types of personal data must also be properly secured to avoid risks like identity fraud and phishing. The DDPA launched its investigation after a tip from a concerned	11 February 2021	DDPA Press Release Link

Development	Summary	Date	Links
	member of the public, reports in the media and two notifications of data breaches by **OLVG** concerning certain staff accessing medical records even though there was no authorization or necessity. After its investigation, the **DDPA** concluded that there are structural shortcomings in the way **OLVG** secures access to medical records. Specifically, it found two violations of the GDPR: – Every time a staff member accesses medical records, these details must be recorded in a log. In addition, the hospital must review this access log regularly, so that it can take timely steps if it finds that someone has accessed a record when they are not actually authorized to do so. **OLVG** did have an automated procedure that logged who accessed which files, but it did not review the logs often enough to check for cases of unauthorized access. – Good security requires two-factor authentication to establish the identity of a user who wants access to a patient record. Examples are a code or password in combination with a personnel badge. **OLVG** did not require two-factor authentication when access was requested from inside the hospital. Access from a location outside the hospital was secured with two-factor authentication. **OLVG** improved its systems security during the DDPA's investigation. The hospital introduced a structural procedure for reviewing access logs, as well as two-factor authentication for access to medical records from inside the hospital. **OLVG** will not file an objection or appeal against the decision of the **DDPA** to impose a fine.		
DDPA demands clarification of Dutch Municipal Health Service regarding large personal data leak	An investigation by a Dutch news channel revealed that personal data of millions of Dutch citizens has been traded on a large scale, originating from two COVID-19 systems of the Municipal Health Service ("**GGD**"). The personal data concerns addresses, telephone numbers, social security numbers and COVID-19 test results. The Dutch Data Protection Authority ("**DDPA**") has demanded immediate clarification from the **GGD** and noted that	27 January 2021	DDPA Press Release Link

Development	Summary	Date	Links
	the **GGD** has to inform data subjects of the data breach as soon as possible. In recent years, the **DDPA** has regularly warned both the government and the healthcare sector about the importance of the security of medical data meeting the highest standards. When testing for COVID-19 and source/contact research, the **GGD** processes data from many subjects. Such personal data includes name, address, place of residence, phone numbers, social security numbers and test results. All this data is up-to-date and accessible in large quantities. Due to the many people involved in testing, source and contact investigations, such data has to be secured extra carefully. Furthermore, it should be monitored that employees do not request or have access to more data than necessary.		

Russian Federation

Contributors

Victoria Goldman
Managing Partner
T: +7 812 363 3377
victoria.goldman@
eversheds-sutherland.ru

Ivan Kaisarov
Senior Associate
T: +7 812 363 3377
ivan.kaisarov@
eversheds-sutherland.ru

Development	Summary	Date	Links
Requirements for providing consent to distribution of personal data have been established	On 1 March 2021, a law amending the Russian Personal Data Law came into force. The amendments set out the requirements for the distribution of personal data to an indefinite circle of persons and establish the concept of "personal data permitted by the subject of personal data for distribution". These provisions apply, inter alia, to the publication of personal data on the Internet, e.g., on corporate websites of companies. The basis for the distribution of personal data is consent, the form of which shall be established by Roskomnadzor. A draft of Roskomnadzor's order on the relevant issue was issued recently. According to the draft order, the consent of the data subject can be provided to the operator directly or by using Roskomnadzor's information system. The subject's consent should include the following information: – surname, name, patronymic (if any) of the subject in Russian – contact information of the subject – name or surname, first name, patronymic (if any) and address of the operator receiving the consent of the subject – the purpose of the data processing – the categories and list of data subject to the transfer for which consent is given – categories and lists of data in relation to which conditions and prohibitions are established, as well as a list of conditions and prohibitions – the term for which the consent is valid	27 January 2021	Text of the draft Link

Development	Summary	Date	Links
	– details of the operator's information distribution platform through which access to the personal data will be provided to an unlimited number of persons		
Fines for infringements of Russian personal data law have been increased	A law amending the Code of Administrative Offenses of the Russian Federation (Administrative Code) came into force at the end of March 2021. This law changes Article 13.11 of the Administrative Code and doubles the fines for administrative offenses relating to personal data. For instance, the processing of personal data that is not provided for by law or is incompatible with the purposes of collection shall entail the imposition of an administrative fine on officials ranging from RUB 10 000 to RUB 20 000 (EUR 110-220) and from RUB 60 000 to RUB 100 000 (EUR 660-1,100) for legal entities. Previously, this offense entailed a warning or a fine of half of the new amounts. The law also introduced fines for repeated offenses. The fines for such repeated violations will range from RUB 20 000 to RUB 50 000 rubles (EUR 220-550) for officials and from RUB 100 000 to RUB 300 000 (EUR 1,100 – 3,300) for legal entities. The fines have also increased for: – processing of personal data without written consent – failure to comply with the obligation to publish or provide access to a personal data processing policy – failure to provide the data subject with information about the processing of his/her personal datafailure to comply with the requirement to clarify, block or destroy personal data – failure to comply with the requirements for ensuring the safety of personal data during its manual processing The new law entered into force on 27 March 2021.	24 February 2021	Text of the Law Link
A list of Russian programs which should be installed on devices and fines for selling devices without such programs have been developed	The law on the compulsory pre-installation of Russian programs onto devices came into force on 1 April 2021. The government has recently approved a list of Russian programs that should be pre-installed on certain devices.	24 March 2021	Text of the Order Link Text of the Law

Development	Summary	Date	Links
	Smartphones and tablet computers will come pre-installed with, inter alia, ICQ, voice assistant "Marusya", VKontakte, Odnoklassniki, MirPay, State Services Russian Federation and Kaspersky Internet Security. The program "MyOffice Standard. Home version" will come pre-installed on computers (except for tablets) and Wink, IVI, KinoPoisk, OKKO and other programs will be pre-installed on TVs with a digital control unit which have the ability to install programs from application stores. Moreover, on 24 March 2021, the President of the Russian Federation signed a law amending Article 14.8 of Code of Administrative Offenses of the Russian Federation concerning liability for the sale of devices without pre-installed Russian software. Fines for officials will range from RUB 30 000 to RUB 50 000 and from RUB 50 000 to RUB 200 000 for legal entities. The new law will enter into force on 1 July 2021.		Link

South Africa

Contributors

Grant Williams
Partner
T: +27 11 575 3647
grantwilliams@
eversheds-sutherland.co.za

Rebecca Hughes
Specialist Consultant
T: +27 10 003 1383
rebeccahughes@
eversheds-sutherland.co.za

Development	Summary	Date	Links
GUIDELINES TO DEVELOP A CODE OF CONDUCT, 15 FEBRUARY 2021, AND NOTICE RELATING TO CODES OF CONDUCT	Guidelines to Develop a Code of Conduct Chapter 3 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (**POPIA**) regulates the processing of personal information by or for a responsible party through compliance with the eight (8) conditions for the lawful processing of personal information. **POPIA** empowers the Information Regulator (**Regulator**) to: – issue, from time to time, codes of conduct, and to amend and revoke codes – make guidelines that would assist bodies to develop or to apply codes – approve codes – consider afresh, upon application, the determinations by adjudicators under approved codes The purpose of a code is to establish a voluntarily accountability tool and to promote transparency for relevant bodies on how personal information should be processed. These guidelines are intended to encourage different sectors to develop codes within an established framework and harmonise the code with **POPIA**. The Regulator has issued these guidelines to: – serve as an explanatory aid to Chapter 7 of **POPIA**	15 February 2021 Effective from 01 March 2021	Guidelines to Develop a Code of Conduct Link Notice relating to Codes of Conduct Link

Development	Summary	Date	Links
	– serve as a practical guide that outlines minimum criteria and provides a framework to ensure that codes are evaluated in a standard manner The relevant bodies bound by an issued code of conduct must refrain from performing an act or engaging in a practice that breaches the code. A breach of an issued code is deemed to be a breach of the conditions for lawful processing of personal information, and will be dealt with in terms of Chapter 10 (Enforcement) of **POPIA**.		
GUIDANCE NOTE ON APPLICATIONS FOR PRIOR AUTHORISATION, 11 MARCH 2021	Guidance Note on Applications for Prior Authorisation POPIA provides that a responsible party must obtain prior authorisation from the Regulator if the responsible party plans to: – process any unique identifiers of data subjects – for a purpose other than the one for which the identifier was specifically intended at collection – with the aim of linking the information together with information processed by other responsible parties – process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties – process information for the purposes of credit reporting – transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information The Regulator has issued this Guidance Note to guide responsible parties who are currently processing or intend to process personal information which is subject to prior authorisation to ensure compliance with the relevant provisions of **POPIA**.	11 March 2021	Guidance Note on Applications for Prior Authorisation Link
GUIDANCE NOTE ON INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS, 1 APRIL 2021 IN TERMS OF THE PROTECTION OF PERSONAL	Guidance Note on Information Officers and Deputy Information Officers **POPIA** prescribes compulsory requirements for the registration of Information Officers with the Regulator in terms of section 55(2) of **POPIA**. Information Officers and Deputy Information Officers	01 April 2021	Guidance Note on Information Officers and Deputy Information Officers

Development	Summary	Date	Links
INFORMATION ACT 4 OF 2013 (POPIA)	may only take up their duties after being registered with the Regulator. Information Officers will be responsible for ensuring that the responsible party for which they have been appointed is compliant with the provisions of **POPIA**. The Regulator has issued this Guidance Note to provide guidance and procedures for the: – obligations and liabilities of Information Officers and Deputy Information Officers – registration of Information Officers with the Information Regulator – updating the details of Information Officers – designation of Deputy Information Officers – delegation of duties and responsibilities of the Information Officers to the Deputy Information Officers Of particular interest is that the Guidance Note specifically states that any person authorised as Information Officer (or Deputy Information Officer) must be a natural person, and an employee of the private body, and that multi-national organisations based outside of South Africa must authorise a person within South Africa as an Information Officer. In light of the broad obligations placed on the Information Officer, the person authorised as an Information Officer should be at an executive level or equivalent position. This means that only an employee of a private body at a level of management and above should be considered for authorisation as an Information Officer of that body.		Link Information Officer's Registration Form Link

Sweden

Contributors

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

Josefine Karlsson
Associate
T: +46 8 54 53 22 00
josefinekarlsson@
eversheds-sutherland.se

Development	Summary	Date	Links
Swedish DPA submits its first privacy protection report to the Swedish government	The Swedish Authority for Privacy Protection (the "**Swedish DPA**") has, on behalf of the Swedish government, submitted its first report on the most current and important developments which can affect privacy rights. The report emphasizes that Sweden's ambitious digitalization policy must be supplemented with equally ambitious goals from a privacy perspective. Artificial intelligence (**AI**) is specifically highlighted as an area that is now cheaper and easier than ever before to use as a means of gathering and analyzing large amounts of data. The report also notes that data gathering technologies which have previously been restricted to the digital world have now through the widespread use of items such as smartphones and training bracelets shifted to the physical space. The **Swedish DPA** is of the opinion that these technological developments pose new risks to privacy protection as parties engaged in data processing are essentially able to gain complete insight surrounding all aspects of a data subject. The **Swedish DPA** has provided suggestions in its report to address these upcoming risks to privacy protection, such as: – supporting research initiatives to further develop techniques for privacy protection – defining clear goals and measures to strengthen – the rights of data subjects and to enable data subjects to control and decide how their personal data is being handled by both companies and public authorities	28 January 2021	Press statement (in Swedish) Link Report (in Swedish) Link

Development	Summary	Date	Links
	The **Swedish DPA** concludes the report with a statement that during the current year they will initiate more audits based on complaints from data subjects.		
Swedish DPA approves binding corporate rules for a Swedish corporate group	The **Swedish DPA** has approved binding corporate rules (**BCR**) for the Swedish group of companies, Elanders. **BCRs** are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. The **Swedish DPA** along with other European data protection authorities have been involved in the approval procedure. The European Data Protection Board has also issued its opinion on the matter.	29 January 2021	Press statement (in Swedish) Link Approval decision (in Swedish) Link EDPB statement Link
Swedish DPA: audits initiated on two Swedish companies for using CCTV in their warehouses	The **Swedish DPA** has initiated audits of two Swedish companies for using CCTV in their warehouses. The audits will primarily focus on whether CCTV is used to monitor and manage the warehouse staff as well as examining if video recording is used. CCTV may not be used for the purposes of managing staff and video recording must only be used under special circumstances such as monitoring theft-prone property or documenting issues related to theft.	11 February 2021	Press statement (in Swedish) Link Audit statement (in Swedish) Link Audit statement (in Swedish) Link
Swedish DPA: police unlawfully used facial recognition app	The **Swedish DPA** has identified that the Swedish Police Authority has processed personal data in breach of the Swedish Criminal Data Act when using Clearview AI to identify individuals. The investigation concluded that Clearview AI had been used by the Police on several occasions. According to the Police a few employees had used the application without any prior authorisation. When using Clearview AI the Police had unlawfully processed biometric data for facial recognition as well as having failed to conduct a data protection impact assessment which this case of processing would require.	11 February 2021	Press statement Link Decision (in Swedish) Link

Development	Summary	Date	Links
	An administrative fine of SEK 2 500 000 was imposed by the **Swedish DPA**. The Police were also ordered to conduct further training and education of their employees, inform the data subjects whose data had been disclosed to Clearview AI under the limitations of confidentiality rules and ensure, to the extent possible, that any personal data transferred to Clearview AI was deleted.		
Swedish DPA: SEK 150 million in administrative fine has been issued during 2020	The **Swedish DPA** has issued a total of SEK 150 million in administrative fines during 2020. During the previous year, 52 audits were initiated and 53 audits were completed of which 15 resulted in administrative fines being issued. The **Swedish DPA** has also during the previous year received 4,600 notifications of personal data breaches, 3,200 complaints from data subjects and made decisions in over 1,000 matters concerning permits to use CCTV. The processing time for permits has also been halved to 6 months. It is also noted that businesses have experienced increasing challenges with being compliant to data privacy laws due to the lack of uniformity in the application of the laws across the member states. The European Commission has called for further harmonization, especially regarding how complaints from data subjects are handled. The **Swedish DPA** intends to initiate more audits going forward and investigate all complaints that are received.	22 February 2021	Press statement (in Swedish) Link Annual report 2020 (in Swedish) Link
Swedish DPA prioritizes audits based on complaints received from data subjects for the next two years	The **Swedish DPA** has adopted a new supervision policy and an audit plan for the coming two years. The new plan focuses on initiating audits based on complaints received by data subjects and will primarily consist of monitoring the application of the General Data Protection Regulation (GDPR).	10 March 2021	Press statement (in Swedish) Link Supervision policy (in Swedish) Link Audit plan (in Swedish) Link

Sweden

Development	Summary	Date	Links
Swedish DPA: online courses available during spring 2021	The **Swedish DPA** will arrange training on the basics of the GDPR.These sessions will be held on 27 May 2021 and 3 June 2021. An advanced course in CCTV will also be arranged, on 25 May 2021.	31 March 2021	Press statement (in Swedish) Link

United Kingdom

Contributors

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

Kirsty Greyling
Associate
T: +44 20 7919 0756
kirstygreyling@
eversheds-sutherland.com

Development	Summary	Date	Links
CMA publishes research on impact of algorithms	The UK Competitions and Market Authority (**CMA**) has published research on how algorithms can reduce competition and harm consumers. As algorithms support many online activities, markets and technology companies, their impact is huge. However as algorithms are developed, transparency is often lost, and it is more difficult to detect when harm is caused. The **CMA's** paper has been launched with a call for information to academics and industry experts, establishing a new work programme to analyse algorithms and help the **CMA** to identify harm caused by algorithms. The **CMA's** paper is summarised as follows: – Direct harms to consumers (often involving personalisation, which is difficult to detect and allows the manipulation of consumer choices) – The use of algorithms to exclude competitors and reduce competition – Techniques to analyse algorithm systems in order to assess whether consumer or competition law is breached – The role of regulators to establish standards and accountability – by supporting best practice and remedying harms The **CMA's** approach highlights the need to identify these areas of harm, but recognises the underlying challenges.	20 January 2021	Press release Research paper

Development	Summary	Date	Links
ICO resumes investigation into adtech industry	After the pandemic halted its investigation last year, the **ICO** have resumed their investigation into the adtech industry and real time bidding. The **ICO** recognises that these industries often need to use personal data to provided targeted advertising and there are concerns that the necessary consents are not currently being obtained, which is a particular worry for the most vulnerable of customers. The **ICO** will carry out a series of audits and issue subsequent notices in the months to come.	22 January 2021	Press release
ICO blog detailing impact of the UK-EU trade agreement on data protection	**ICO** have published a blog which details the impact of the UK-EU trade agreement on data protection within the UK. They note the provisions which commit both parties to the long term protection of data and continued collaboration to ensure standards remain high. Further, the **ICO** highlights the ongoing ability for the EU to transfer data to the UK, at least for the next four months, without restriction while an adequacy decision is reached. The **ICO** recommends that businesses take reasonable steps to ensure that they remain compliant and up to date with developments, noting that new **SCCs** are due to be approved in the coming months.	22 January 2021	Press release
DCMS publishes trust framework relating to the use of digital identities	The UK Department of Culture, Media and Sport ("**DCMS**") has published a draft 'trust framework' to govern the future use of digital identities, as part of a wider aim to allow people to quickly and efficiently verify their identities using modern technology. The draft framework requires organisations providing or using digital identity services to: – Have a data management policy – Follow industry standards and best practice for information security and encryption – Inform the user if any changes are made to their digital identity	11 February 2021	Press release Policy paper Response survey

Development	Summary	Date	Links
	– Have a detailed account recovery process and inform users if fraudulent access or use of their account is suspected – Follow guidance on how to choose secure authenticators – Organisations must publish an annual report explaining if and why demographic groups have been excluded from their service Public comments were invited until 11 March 2021. This feedback will shape the next iteration of the framework. Once finalised, it is expected that the framework will become law.		
ICO launches data analytics toolkit	The **ICO** has launched a data analytics toolkit, designed to be used by organisations to highlight the risks to the rights and freedoms of individuals posed by data analytics. The **ICO** has highlighted that the toolkit is not a guarantee of absolute compliance with **DP** law, but a starting point. **ICO** guidance on explaining decisions made with **AI** (published together with the Alan Turing Institute) and on **AI** and **DP** should be used to supplement the toolkit. The toolkit follows four themes: – lawfulness – accountability and governance – DP principles – data subject rights Organisations use the toolkit by answering a series of questions under the above themes; a report is then produced with tailored guidance for the particular data analytics project. This should be used together with advice from the relevant **DPO**.	18 February 2021	Toolkit
EU publishes Draft UK Adequacy Decision	On 19 February the European Commission began the process in adopting adequacy decisions for the transfers of personal data to the UK under the General Data Protection Regulation (Regulation (EU) 2016/679) and under the Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680)	19 February 2021	Press release GDPR draft decision Law Enforcement Directive draft decision

Development	Summary	Date	Links
	The Commission have looked at the UK's approach to personal data protection and had decided that an equivalent level of protection is offered in both of the laws above. Once adopted the decisions will be valid for four years after which it will be reviewed and renewed so long as the UK maintains appropriate levels of protection. Further to the announcement, the European Data Protection Board published its opinion on the TCA and an agreement on the security procedures for exchanging and protecting classified information.		
Secretary of state for DCMS publishes an article on the future of Data Protection in the UK post Brexit	On 27 February 2021, Oliver Dowden, the Secretary of state for the Department for Digital, Culture, Media and Sport ("**DCMS**"), published an article in the Financial Times setting out a new approach to data in light of the appointment of a new Information Commissioner in October 2021. Mr Dowden states that he wants the rhetoric around the use of data to shift from primarily focussing on privacy to a focus on securing personal information whilst also enabling data to be used in order to further economic and societal objectives. Mr Dowden writes that by diverging from the GDPR, the UK can achieve this shift in approach. According to Mr Dowden, the appointment of a new Information Commissioner will help to foster this new approach to data in the UK. Mr Dowden writes that he will soon announce the UK Government's priority countries for data adequacy agreements.	27 February 2021	Article
DRCF publishes its first yearly plan of work	The Digital Regulation Cooperation Forum ("**DRCF**") has published its first yearly plan of work, covering 2021/22. The **DRCF** was established in July 2020 by the **CMA**, **ICO** and Ofcom. Its goal is to provide a higher level of cooperation between these organisations in the context of regulating online platforms. The FCA is currently an observer member of **DRCF**, and will join as a full member in April 2021. The **DRCF** will focus on three priority areas during 2021/22:	10 March 2021	Press release (CMA) Press release (ICO) Plan

Development	Summary	Date	Links
	– responding strategically to industry and technological developments – developing joined-up regulatory approaches – building shared skills and capabilities		

United States

Contributors

Michael Bahar
Partner
T: +1 202.383.0882
michaelbahar@
eversheds-sutherland.com

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

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

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

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

Development	Summary	Date	Links
The Federal Trade Commission (FTC) signaled increased focus on commercial collection and use of biometric data.	In a major development for companies that collect, use, and store biometric data, the US Federal Trade Commission (**FTC**) reached a proposed settlement of a complaint against a company that allegedly deceived consumers about its use of facial recognition technology and its retention of consumers' biometric data. In its January 11, 2021 announcement of a settlement with the parent company of a now-defunct photo storage app, the **FTC** signaled that it is increasing its focus on commercial practices relating to consumer biometric information. As part of the settlement, the defendant was required to delete facial recognition algorithms created using photographs provided by consumers without their consent. The settlement is also noteworthy in light of the enormous recent and projected growth of the biometric industry, the small minority of states that directly regulate private entities' collection and use of this data, and one Commissioner's recent public comments about the **FTC's** interest in policing this area.	11 January 2021	Agreement Containing FTC Consent Order

Development	Summary	Date	Links
The FTC settled with Flo Health, Inc. regarding its misleading privacy and data sharing practices.	On January 13, 2021 the **FTC** announced its settlement with Flo Health, Inc. over allegations that it misled users about the disclosure of their sensitive health information. The proposed terms of the FTC's consent order would prohibit Flo Health from misrepresenting: (1) the purposes for which it or the entities to whom it discloses data collect, maintain, use or disclose the data; (2) the degree of control its users have over the company's data uses; (3) the company's compliance with any privacy, security or compliance program; and (4) how the company collects, maintains, uses, discloses, deletes or protects users' personal information. Flo Health would also be required to notify affected users about the unauthorized disclosure of their health information, obtain express consent from its users before sharing health information with any third party, and instruct any third party that received users' health information to destroy such data within 30 days after the order is filed.	13 January 2021	Agreement Containing FTC Consent Order
The National Institute of Standards and Technology (NIST) announced its cybersecurity and privacy priorities for 2021.	NIST published an article detailing the specific cybersecurity and privacy concerns that the consortium will seek to address in 2021 and the years ahead. Specifically, **NIST** identified nine priority areas for the next several years: enhancing risk management; privacy, strengthening cryptographic standards and validation (especially in response to advances in quantum computing); cybersecurity awareness, training, and education and workforce development; metrics and measurements; identity and access management; trustworthy networks; trustworthy platforms; and securing emerging technologies.	2 February 2021	NIST Article
The New York Department of Financial Service (NY DFS) issued cyber insurance risk framework.	In Circular Letter No. 2, the NY DFS introduced a cyber insurance risk framework directed to New York-regulated property/casualty insurers that outlines best practices for managing cyber insurance risk. The frameworks is the first of its kind; no other U.S. regulator has issued guidance of this nature on cyber insurance. The framework details seven best practices for insurers: (1) establish a formal cyber insurance risk strategy; (2) manage and eliminate exposure to "silent" cyber risk; (3) evaluate systemic risk; (4) rigorously measure insured risk; (5) educate insureds and insurance producers about cybersecurity; (6) obtain cybersecurity expertise; and (7) require victims to notify law enforcement.	4 February 2021	Circular Letter No. 2

Development	Summary	Date	Links
The Eleventh Circuit held that future risk of identity theft in a data breach suit does not establish standing.	In Tsao v. Captiva MVP Restaurant Partners LLC, the Eleventh Circuit held that a plaintiff had not established standing to sue for a data breach because it failed to demonstrate substantial risk for future identity theft arising out of unauthorized access to credit card numbers. The court noted that while "evidence of actual misuse is not necessary ... to establish standing following a data breach," a named plaintiff in a class action must provide "specific evidence of some misuse of class members' data" to show that there is a "certainly impending" harm of future identity theft or that such harm is of "substantial risk." The court also noted that the injuries plaintiff alleged were inextricably tied to his perception of the "insubstantial, non-imminent risk of identity theft." Relatedly, the pending decision in U.S. Supreme Court case TransUnion LLC v. Ramirez will shed additional light on whether a "material risk of harm" is sufficient to confer standing.	4 February 2021	The Eleventh Circuit's Decision
The First Circuit Court of Appeals confirmed government's expansive authority to search electronic devices.	In a closely watched decision, the U.S. Court of Appeals for the First Circuit confirmed the government's expansive authority to search cell phones, laptops, and other electronic devices at the border. On February 9, 2021, the First Circuit held that the U.S. Department of Homeland Security's internal policies for searching individuals' electronic devices when they travel across the US border are constitutional. Under the precedent set by Alasaad v. Wolf, border agents can (i) search electronic devices without a warrant or probable cause; (ii) conduct certain types of searches even if they do not have reasonable suspicion; (iii) search electronic devices for evidence of contraband or other crimes enforced by the U.S. Department of Homeland Security (DHS); and (iv) detain an electronic device after the traveler crosses the border.	9 February 2021	The First Circuit's Decision
Virginia became the second state to adopt a comprehensive privacy law.	On March 2, 2021, Governor Northam signed the Virginia Consumer Data Protection Act (**CDPA**) making it the country's second comprehensive data privacy legislation following California's Consumer Protection Act of 2018. It is unlikely to be the last, emphasizing the importance for companies to adopt and maintain a proactive and comprehensive data strategy. Set to take effect on January 1, 2023, the **CDPA** requires businesses to make significant changes to their privacy policies	2 March 2021	Consumer Data Protection Act

Development	Summary	Date	Links
	and to provide covered consumers with substantial rights. Note that the Virginia Attorney General's office will be the sole enforcement authority as the Act does not provide a private right of action for consumers.		
Then-California Attorney General Becerra announced new regulations to enhance the California Consumer Privacy Act (CCPA) consumer opt-out right.	On March 15, 2021, then-California Attorney General Xavier Becerra announced a fifth set of new regulations that modified the **CCPA**. The regulations, which were approved by the Office of Administrative Law, fortify California consumers' rights to opt out of the sale of their personal information by prohibiting the use of so-called "dark patterns." "Dark patterns" are generally described as deliberate attempts to subvert or impair a consumer's choice to opt out; they may be used deceive the consumer into granting knowing consent. The regulations, which took effect the same day, ban the use of the following "dark patterns": – Using an opt-out request process that requires more steps than the process for a consumer to opt back into the sale of personal information after previously opting out – Using confusing language (e.g., double-negatives, "Don't Not Sell My Personal Information") – Requiring consumers to click through or listen to unnecessary reasons why they should not submit a request to opt-out before confirming their request – Requiring a consumer to provide personal information that is unnecessary to implement an opt-out request – Upon clicking the "Do Not Sell My Personal Information" link, requiring a consumer to search or scroll through the text of a website or privacy policy to submit the opt-out request.	15 March 2021	CCPA Additional Amendments

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

Kirsty Greyling
Senior Associate
T: +44 20 7919 0756
kirstygreyling@eversheds-sutherland.com

Harriet Bridges
Trainee Solicitor
T: +44 1223 44 3644
harrietbridges@eversheds-sutherland.com

Tom Charnock
Trainee Solicitor
T: +44 20 7919 4915
thomascharnock@eversheds-sutherland.com

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

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

eversheds-sutherland.com

CAM_1B\7415707\1