



Update

Your quarterly Data Privacy and
Cybersecurity update

January to March 2020



Executive summary



Welcome to the seventh edition of Udata!

Udata 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 2020 and is full of newsworthy items from our team members around the globe, including:

- A special edition **chapter** on Coronavirus Updates from our colleagues around the globe, from developments in **China** in relation to [using big data for prevention and control](#), [emergency measures](#) in **Italy** to protect workplaces, [data sharing notifications for companies](#) being issued in the **UK**, [potential tracking of COVID-19 carriers](#) in **Hong Kong** to the **EU** issuing guidance on [remote working](#), [how to protect yourself from cyberattacks](#) and [misinformation](#);
- From our general updates - regulators in the **Netherlands** and **Spain** confirm AI to be a key focus, with guidance released in [Spain on data processing in the AI lifecycle](#), and a [regulatory framework issued in the Netherlands](#);
- The **CNIL** has released detailed [recommendations on the meaning of consent](#) in the context of cookies; and
- Developments in the **USA** see the [California Privacy Rights Act expand upon the CCPA](#).

You can also read our [Spotlight On...](#) briefings, which provide more in depth analysis of particular topics such as: Data Protection Implications for Organisations in Ireland during COVID-19, Bitcoin as Property following a ransomware attack, what accessibility means under the CCPA, Biometrics litigation in healthcare and the US cybersecurity and data privacy review – looking back on 2019 and ahead for 2020.

We hope you enjoy reading this edition.

Follow us on Twitter at:



@ESPrivacyLaw



Paula Barrett

Co-Lead of Global Cybersecurity and Data Privacy

T: +44 20 7919 4634

paulabarrett@

eversheds-sutherland.com



Michael Bahar

Co-Lead of Global Cybersecurity and Data Privacy

T: +1 202 383 0882

michaelbahar@

eversheds-sutherland.com

Coronavirus Updates

General EU and International

Austria

China

France

Germany

Hong Kong

Hungary

Ireland

Italy

Lithuania

Malaysia

Mauritius

Netherlands

Poland

Russian Federation

Singapore

South Africa

Spain

Sweden

United Arab Emirates

United Kingdom

United States



Coronavirus Updates



General EU

Contributors



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



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

Development	Summary	Date	Links
EDPS Data Strategy for 2020-2024 delayed until May 2020, due to the coronavirus (COVID-19) outbreak	<p>The European Data Protection Supervisor (“EDPS”) has delayed the publication of his 2020-2024 strategy because of the coronavirus situation. The strategy was due to be released on 19 March 2020 but will be postponed until May.</p> <p>Mr Wiewiórowski stated that the EDPS strategy is designed to be adaptable to global game changers and that the coronavirus outbreak clearly falls within this category. The EDPS strategy for the next five years needs to be re-considered in light of the changes and questions which the coronavirus outbreak raises in relation to individuals’ fundamental rights and the crucial principles which are to govern our interconnected lives.</p>	20 March 2020	Press release Link
ENISA shares cybersecurity tips for remote working during COVID-19	<p>The executive director of the European Union Agency for Cybersecurity (“ENISA”), Juhan Lepassaar has shared cybersecurity tips for those working from home during the COVID-19 pandemic. He highlighted several fundamentals such as:</p> <ul style="list-style-type: none"> – Ensuring you have a secure wifi connection, a fully updated anti-virus system, up-to-date security software and encryption tools. – Remembering to back up all important files periodically – Locking your computer screen if you are working from a shared space. <p>He also shared several tips for employers to ensure cybersecurity in their systems:</p>	24 March 2020	Press release Link



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – Share regular feedback to staff on how to react to problems (i.e. emergency contacts, hours of service) – Prioritise appropriately the support of remote access solutions. Employers should provide at least authentication and secure session capabilities (essentially encryption). – Provide virtual solutions such as e-signatures and virtual approval workflows. – Ensure adequate support in case of problems set out clear procedures to follow in case of a security incident. – Where possible, consider restricting access to sensitive systems. <p>He advised on being wary of COVID-19 related phishing attempts and shared the following preventative steps:</p> <ul style="list-style-type: none"> – Where possible, keep work and leisure activities limited to separate devices – Exercise caution when opening any mails referring to COVID-19 – Be careful when responding to any emails asking to check or renew credentials, even if sent from a trusted source. Verify authenticity through other means. <p>Be wary of e-mails from people you do not know especially if they ask to connect to links or open files or e-mails creating a sense of urgency and severe consequences (if in doubt check with your security officer).</p>		
EU planning use of telecoms data to map spread of coronavirus	<p>In response to the COVID-19 outbreak, the EU Commission has held discussions with European telecommunications companies and the Global System for Mobile Communications Association ("GSMA") to see whether anonymised smartphone location data could be used for modelling and predicting the spread of the virus. Internal Market Commissioner, Thierry Breton, has stated that the data can be used in a manner compliant with the GDPR and e-Privacy legislation.</p>	24 March 2020	<p>Announcement</p> <p>Link</p>



Development	Summary	Date	Links
	Additionally, all parties also acknowledged the importance of protecting the networks against cyber-attacks and agreed to further discussions to explore solutions.		
EDPS publishes its response to the Directorate General for Communications Networks, Content and Technology ("DG CONNECT"), on monitoring the spread of COVID-19	<p>The EDPS Wojciech Wiewiórowski, shared his response to the Directorate-General for Communications Networks, Content and Technology ("DG CONNECT"), via Letter addressing ongoing discussions the European Commission is having in some Member States with telecommunications providers, with the objective of using data to track the spread of COVID-19.</p> <p>The Letter outlines that EU data protection rules are flexible enough to allow for various measures to be taken in the fight against pandemics and stressed the importance of full transparency to the public on the purpose and procedure of future measures. The Letter also included the following recommendations:</p> <ul style="list-style-type: none"> – Data anonymisation: In relation to only using anonymous data to map population movements, the EDPS cautioned that effective data anonymisation comprises more than removing obvious identifies such as phone and IMEI numbers. – Data security and access: the EDPS stressed the importance of applying adequate measures to ensure secure transmission of data from the telecoms providers. Access of the data should also be limited to authorised experts in spatial epidemiology, data protection and data science. – Data retention: Data should be deleted as soon as the current emergency ends. 	25 March 2020	Letter Link
Council of Europe issues statement on coronavirus and cybercrime	The Council of Europe ("Council") issued a statement on cybercrime in the COVID-19 pandemic. The statement highlights a range of digital vulnerabilities being exploited by malicious actors, including: phishing campaigns and malware distribution through seemingly genuine websites and documents offering information on COVID-19; ransomware shutting down health-related facilities in order to extort ransom; attacks on critical infrastructures such as the World Health Organisation; targeting of mobile devices via apps, to extract payments; unauthorised access to computer systems via teleworking employees; fraud	27 March 2020	Statement Link



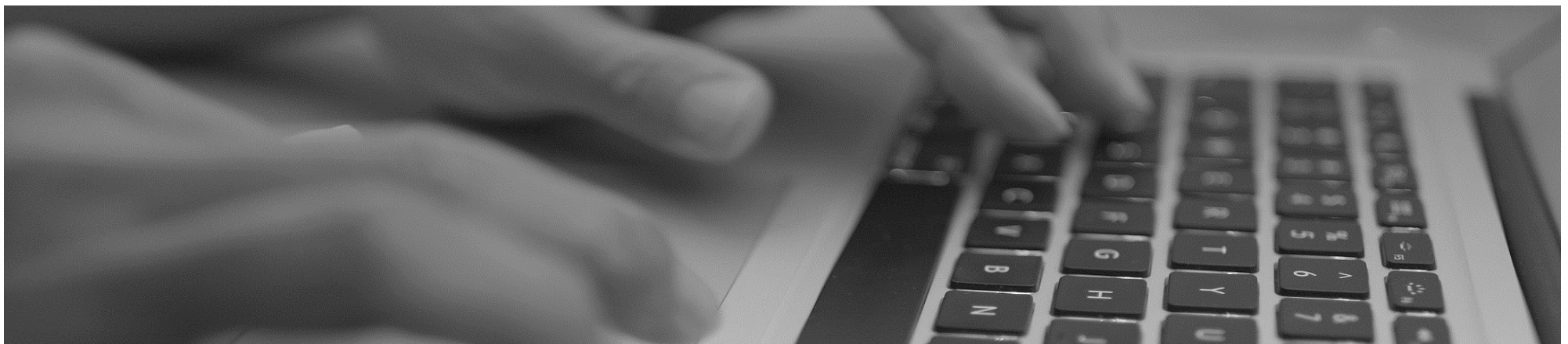
Development	Summary	Date	Links
	<p>schemes involving the sale of fake COVID-19 related treatments and products; and the spread of misinformation (fake news) to create panic, social instability and distrust in governments and health authorities.</p> <p>The Council advises the public to take extra caution and reinforce security measures, and highlights specific resources published by Europol and the ENISA.</p> <p>The Council also states that “additional solutions are required to address future crises”, noting that the 2nd Additional Protocol to the Bucharest Convention, which is currently under negotiation, will facilitate cooperation in urgent situations.</p>		
Council of Europe release statement on data protection and coronavirus	<p>Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe published a statement on data protection and COVID-19.</p> <p>The statement explains that Convention 108 for the protection of individuals with regard to automatic processing of personal data provides high standards of protection for personal data which are compatible with other fundamental rights and public interests. The statement goes on to emphasise the importance of processing personal data in accordance with the data protection principles and contains practical commentary on the application of data protection law to: the processing of health-related data; large-scale data processing; data processing by employers; mobile, computer data and data processing in educational systems.</p> <p>In addition, the statement underlines that data protection rights are not incompatible with epidemiologic monitoring, because anonymised data is not in scope of data protection law, and that the use of aggregate location data to signal gatherings infringing confinement requirements or to indicate movements of persons traveling away from a severely impacted area would therefore not be prevented by data protection requirements.</p> <p>The statement expresses that where restrictions are applied, they must be taken solely on a provisional basis and only for a period of time explicitly limited to the state of emergency. Specific safeguards should be put in place and reassurances should be</p>	30 March 2020	<p>Press release</p> <p>Link</p> <p>Statement</p> <p>Link</p>



Development	Summary	Date	Links
	given that full protection are afforded to personal data once the state of emergency is lifted. The Council invites data protection authorities to carefully assess the measures taken by state authorities in this respect.		
ENISA recommendations for consumers and SMEs for buying and selling online during COVID-19 pandemic	<p>ENISA published its: “<i>Tips for cybersecurity when buying and selling online</i>” following a surge in e-commerce during the coronavirus (COVID-19) pandemic.</p> <p>The recommendations for consumers include: ensuring a secure connection by looking out for website security seals (the presence of a little green padlock); being on guard against phishing scams and fake websites; checking online accounts and your bank statements regularly for fraudulent activity and reporting any suspicious activity to your bank; updating systems with the latest antivirus and antimalware installations; and using strong passwords and avoiding sharing personal information with unknown third parties.</p> <p>The recommendations for SMEs include: securing websites against security threats (including for example enabling two factor authentication); protecting assets by embedding a robust security policy alongside necessary technical and organisation security measures; storing password credentials securely (using techniques such as keyed or salted hashes, where applicable); ensuring compliance with data protection requirements; and monitoring and responding to security incidents.</p>	31 March 2020	<p>Press release</p> <p>Link</p>
EU Parliament issues guidance on how to protect yourself against cyber-attacks during the coronavirus pandemic	<p>The EU Parliament has published online guidance on how people can better protect themselves against cyber-attacks and cybercrime during the current coronavirus pandemic. In particular, it provides information on what the most common form of cyber-attacks are, from fake messages which include malware, fake messages from providers which require your login details and fake messages about packages that do not exist.</p> <p>The website provides guidance on how you can protect yourself online and lists a number of points to consider. These are as follows:</p>	1 April 2020	<p>Recommendations</p> <p>Link</p>



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – be cautious with unsolicited emails, text messages and phone calls; – ensure home networks are secure (limit devices and change passwords); – ensure you have a strong, complex password, and if not change it to a stronger one; – protect equipment (hardware/ software) with updated antivirus software; and <p>do not let family or others use work devices – which is in line with many working from home policies issued by companies to their employees.</p>		
EU Commission launches dedicated website to help address online false claims about COVID-19	<p>The European Commission (“EC”) has responded to the flurry of online false claims and fake news which have been seen during the coronavirus pandemic, by launching a dedicated website. The website provides users with an opportunity to check the facts, learn about online scams and access educational resources and tools. The website also features a video of the President of the EC Ursula von der Leyen, who discusses a few examples of the types of false claims being made and their detrimental effect. Ursula von der Leyen makes clear that the EC is closely monitoring the actions taken by social media platforms at this time.</p>	1 April 2020	<p>Commission response</p> <p>Link</p>





Austria

Contributors



Georg Roehsner
Partner

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



Manuel Boka
Senior Associate

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
Guidelines for Data Processing during the COVID-19 crisis	<p>The Austrian Data Protection Authority (“DPA”) has published guidelines for the processing of personal data in the context of the current COVID-19 crisis.</p> <p>The DPA clarified that data about infections and suspected infections with the SARS-CoV-2-Virus are special categories of data under Article 9 General Data Protection Regulation 2016/679 (“GDPR”). This data may be processed insofar as it is necessary to prevent the spread of the virus and to protect others. Employers can base this processing with regard to their employees (insofar as necessary) on Article 9 (2b) and (2h) GDPR and the transfer of such data to health authorities can be based on Article 9 (2i) GDPR and s 5(3) of the Austrian Epidemic Act.</p> <p>Employers are also entitled to process employees’ private contact details for the purpose of contacting them in case of an infection in the company. However, employees are not obliged to disclose this data to their employer.</p> <p>The DPA reminds companies that all these data must be deleted after the end of the pandemic pursuant to the principle of storage limitation.</p>	17 March 2020	Information by DPA (in German) Link



China

Contributors



Jack Cai
Partner

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



Sam Chen
Senior Associate

T: +86 21 61 37 1004
samchen@
eversheds-sutherland.com



Jerry Wang
Associate

T: +86 21 61 37 1003
jerrywang@
eversheds-sutherland.com

Development	Summary	Date	Links
<p>Notice by the Office of the Central Cyberspace Affairs Commission of Effectively Protecting Personal Information and Using Big Data to Support Joint Prevention and Control (the “Notice”)</p> <p>《中央网络安全和信息化委员会办公室关于做好个人信息保护利用大数据支撑联防联控工作的通知》</p>	<p>On 4 February 2020, the Office of the Central Cyberspace Affairs Commission issued the Notice (with immediate effect) regarding data protection in COVID-19 contingency measures. The Notice is summarised as follows:</p> <ul style="list-style-type: none"> – All regions and departments prioritise the protection of personal information. Unauthorised entities may not unlawfully collect any personal information on the grounds of pandemic prevention and treatment; – The collection of personal information necessary for joint prevention and control should be done with reference to the national standards and adhere to the principle of minimum scope on data subject selection; – Personal information collected for purposes of epidemic prevention and treatment must not be used or disclosed for any other purpose, except in certain circumstances; – Institutions that collect or have control of personal information should be vigilant to data security and unauthorised use; – Under the guidance of relevant departments, capable enterprises are encouraged to actively use big data to analyse and predict the movements of key persons who are 	4 February 2020	<p>Notice by the Office of the Central Cyberspace Affairs Commission of Effectively Protecting Personal Information and Using Big Data to Support Joint Prevention and Control (in Chinese)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>either confirmed, suspected, or have been in close contact with those who are infected; and</p> <p>Breaches of rules and laws in the collection, use, or disclosure of personal information should be reported to the departments of internet information or public security.</p>		





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 Lehuby
Associate

T: +33 1 55 73 42 09
camillelehuby@
eversheds-sutherland.com



Camille Larreur
Associate

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

Development	Summary	Date	Links
Recommendations from the CNIL in the context of COVID-19	<p>The CNIL has issued some recommendations for employers in the context of the COVID-19 crisis.</p> <p>In particular, the CNIL highlights that employers must refrain from collecting information intended to search for possible symptoms of employees and their relatives in a systematic and generalised manner, or through individual inquiries and requests.</p> <p>It is therefore not possible to implement, for example:</p> <ul style="list-style-type: none"> – mandatory body temperature readings of each employee/visitor to be sent daily to the management; – collection of medical records or questionnaires from all employees. – Instead, employers may: – Raise awareness and invite employees to provide information concerning them in relation to possible exposure, either to the employer or to the competent health authorities; – facilitate the transmission of such information by setting up, if necessary, dedicated channels; 	6 March 2020	<p>CNIL statement (in French)</p> <p>Link</p>



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – promote remote working methods; <p>establish a “Business Continuity Plan” to maintain the organisation’s critical business, including measures to protect the safety of employees, identify the essential activities to be maintained and the personnel needed to implement continuity of service.</p>		
SMS sent by the French government to all citizen about COVID-19: applicable legal framework	<p>Following the French President’s speech on 16 March 2020, many French people received a text message reminding them of the safety instructions to be applied to combat the spread of COVID-19. The message raised questions from individuals with regard to the protection of their personal data. The CNIL clarified the legal framework applicable to this type of communication.</p> <p>Article L. 33-1 of the French Post and Electronic Communications Code requires telecommunications operators to broadcast to their subscribers, messages from public authorities intended to warn the population of imminent danger or a major disaster.</p> <p>Therefore, no telephone number was transmitted to the government: the government simply sent a message to the operators who forwarded it to the individuals listed in their databases.</p> <p>The CNIL also confirmed that this arrangement is compliant with the GDPR which allows the use of personal data without consent, particularly in the context of a legal obligation, public interest or for the protection of people’s vital interests.</p>	19 March 2020	<p>CNIL statement (in French)</p> <p>Link</p>



Germany

Contributors



Alexander Niethammer
Partner

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



Lutz Schreiber
Partner

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



Nils Müller
Principal Associate

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



Constantin Herfurth
Associate

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



Sara Ghoroghy
Associate

T: +49 40 80 80 94 446
saraghoroghy@
eversheds-sutherland.com



Philip Kuehn
Associate

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

Development	Summary	Date	Links
DSK gives advice on Data Protection in light of Corona	The DSK (Joint Committee of all Independent German Data Protection Authorities on Federal and State Level) released information for employers on how to handle personal data of employees, guests and visitors in light of the ongoing COVID-19 Pandemic. The DSK clarified that the protection of personal data does not go against measures to mitigate the infection. Even if the processing of health data is in principle only possible on a restrictive basis, data may be collected and used for various measures to contain the coronavirus pandemic or to protect employees in accordance with data protection regulations. The principle of proportionality and the legal basis must always be observed.	13 March 2020	DSK statement Link



Development	Summary	Date	Links
Data Protection Authority of Baden-Württemberg releases information regarding the handling of Corona Cases in the context of Data Protection	The Data Protection Authority of Baden Württemberg has issued some FAQs regarding the handling of Corona cases in the context of data protection. Such questions included on what type of data can be processed or collected if an employee has been or is in contact with a person from a risk region, or if actual contact information can be collected to contact them on a short term notice to stay at home.	13 March 2020	FAQ by the Data Protection Authority of Baden Württemberg 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



Duncan Watt
Consultant

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



Rhys McWhirter
Consultant

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



Wing Chan
Senior Associate

T: +852 2186 3223
wingchan@eversheds-
sutherland.com



Jamie Leung
Solicitor

T: +852 2186 4987
jamieleung@
eversheds-sutherland.com



Phillip Chow
Associate

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



Maggie Lee
Trainee Solicitor

T: +852 2186 4986
maggielee@eversheds-
sutherland.com

Development	Summary	Date	Links
The Privacy Commissioner for Personal Data condemns and provides updates on doxxing	The Privacy Commissioner for Personal Data ("PCPD") noted that frontline medical personnel are being doxxed during the CoVID-19 outbreak, resulting in these personnel experiencing	26 January 2020	Media statement Link



Development	Summary	Date	Links
	<p>unwarranted pressure and fear. The PCPD reiterated that doxxing activities are not only criminal offences under the PDPO, but also violate data ethics and against public interest. The PCPD further urged the doxxers to stop these illegal and irresponsible activities and the operators of the online social platforms to remove the postings without delay.</p> <p>The office of the PCPD has initiated an investigation and written to the overseas data protection authority whose jurisdiction covers the offending platforms for collaborative efforts to combat doxxing activities. In addition, while the PCPD does not have the relevant legal standing to initiate legal proceedings, the affected medical practitioners and their institutions may consider seeking an injunction from the court.</p>		<p>Media statement Link</p> <p>Media statement Link</p>
The Privacy Commissioner for Personal Data responds to privacy issues arising from COVID-19 prevention and control measures	<p>In considering various privacy issues arising from the Government's prevention and control measures against COVID-19, the PCPD has clarified that the absolute right to life and the interests of the public as a whole precede data privacy right of individuals. Generally, Data Protection Principle 3 of the PDPO prohibits the use of data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject's consent. However, in circumstances where the application of the restrictions on the use of personal health data would likely cause serious harm to the health of the data subject (e.g. potential virus carrier) or any other individual, the data user (e.g. Government) may be exempted from such restrictions.</p> <p>In particular, the PCPD noted that while a high degree of privacy is expected for location data of persons under quarantine, ensuring effective quarantine with the aid of video calls and sharing of data is for a lawful purpose of protecting public health and the data collected is not excessive for such purpose. Similarly, the PCPD found that there are sufficient and justifiable legal bases for the Government to collect and use information on social media for the purpose of tracking potential COVID-19 carriers.</p>	12 February 2020	<p>Media statement Link</p> <p>Media statement Link</p>



Hungary

Contributors



Ágnes Szent-Ivány
Partner

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



Katalin Varga
Partner

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



Kinga Mekler
Associate

T: +36 1 394 31 21
mekler@
eversheds-sutherland.hu

Development	Summary	Date	Links
The information letter of the NADP on processing data related to the coronavirus epidemic (NAIH/2020/2586)	The Hungarian National Authority for Data Protection and Freedom of Information issued an information letter on processing data related to the coronavirus. The letter provides guidance on how controllers and processors can develop compliant data processing practices, and ensure the efficient protection of the privacy of data subjects.	10 March 2020	Information letter (in Hungarian) Link Information letter (in English) Link



Ireland

Contributors



Marie McGinley
Partner

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



Fiona Lipsett
Solicitor

T: +35 31 64 41 47 0
fionalipsett@
eversheds-sutherland.ie



Neasa Ní Ghráda
Senior Associate

T: +35 31 66 44 25 8
neasanighrada@
eversheds-sutherland.ie

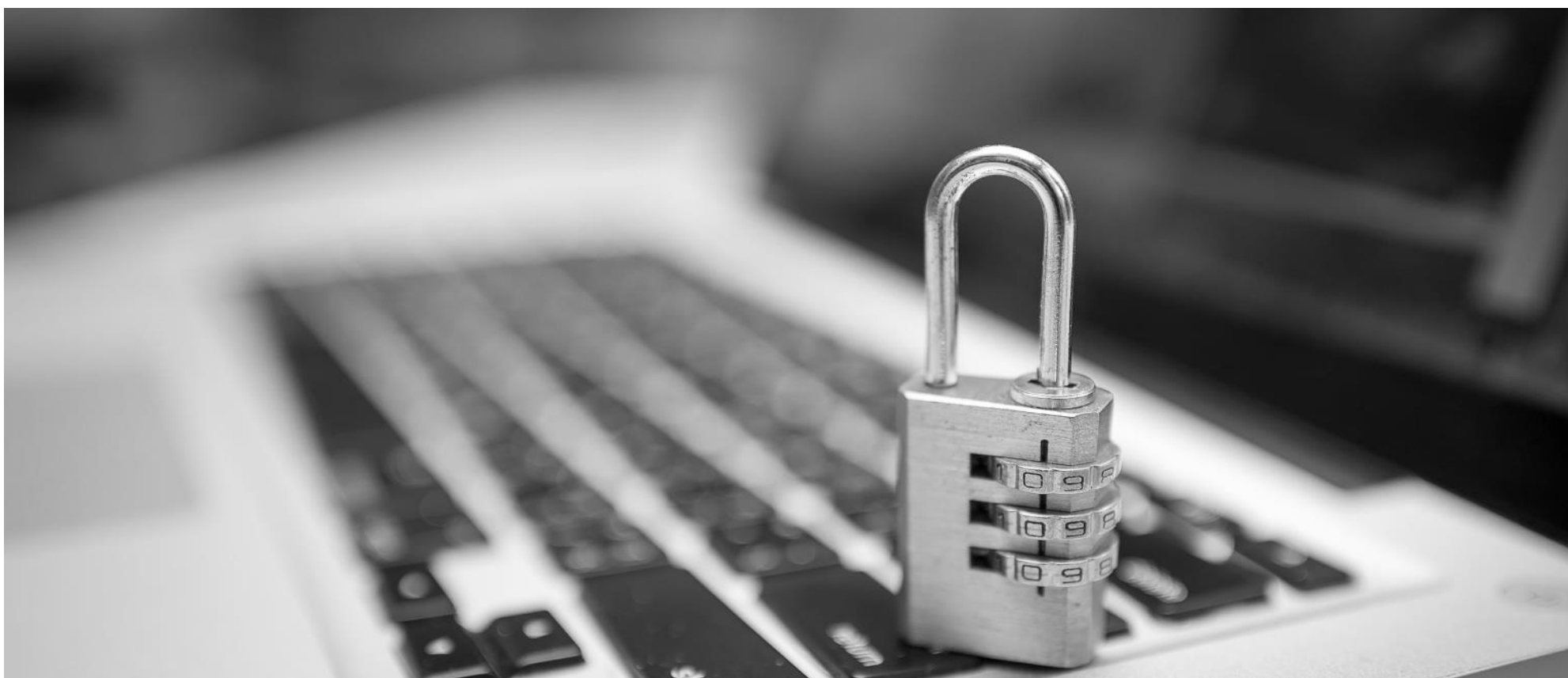
Kirsty Farrell
Trainee

T: +35 3 16 64 49 41
kirstyfarrell@
eversheds-sutherland.ie

Development	Summary	Date	Links
DPC posts blog on data protection and COVID-19	<p>The Data Protection Commission (“DPC”) sought to address the potential data protection issues that may arise when Governments and private, public and voluntary organisations seek to take necessary steps to contain, mitigate and prevent the spread of COVID-19. This may involve the processing of personal and special category data. The DPC has said that “Decisions in this regard should be informed by the guidance and/or directions of public health authorities, or other relevant authorities”.</p> <p>See our article on the Data Protection implications of COVID-19.</p>	6 March 2020	<p>DPC guidance Link</p> <p>Eversheds Sutherland article Link</p>
DPC posts blog on protecting personal data when working remotely	<p>This blog post acknowledged the increase in employees working remotely in efforts to contain and prevent further spread of COVID-19. In order to ensure employees working remotely ensure an adequate level of data protection, the DPC provided a number of tips to keep personal data safe when working away from the office. This includes guidance on devices, emails and cloud and network access.</p>	12 March 2020	<p>DPC guidance Link</p>
DPC posts blog on COVID-19 and data subject access requests (DSARs)	<p>In this blog post, the DPC acknowledged the potential significant impact of COVID-19 on organisations’ ability to comply with DSARs. It noted that while the timeline is prescribed by GDPR and</p>	25 March 2020	<p>DPC guidance Link</p>



Development	Summary	Date	Links
	can't be changed by the DPC, it does recognise the potential for unavoidable delays.		
DPC provides guidance on how to stay safe online during the pandemic	The DPC acknowledged that in a "rapidly changing environment" it is crucial that steps are taken to ensure safety in online interactions. The DPC set out a number of helpful tips on how to stay safe online and how to ensure that personal data, particularly health data and other sensitive data is only shared with and accessed by trusted recipients.	26 March 2020	DPC guidance Link





Italy

Contributors



Massimo Maioletti
Partner

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

Edoardo Coia
Trainee

T: +39 06 89 32 70 34
edoardocoia@
eversheds-sutherland.it

Development	Summary	Date	Links
IDPA's press release on Coronavirus	<p>The Italian Data Protection Authority ("IDPA") issued a press release in relation to data protection considerations when collecting data relating to employees and visitors' COVID symptoms or their recent travel movements.</p> <p>The IDPA stressed that:</p> <ul style="list-style-type: none"> – preventing the spread of Coronavirus is a key objective; – The investigation into and collection of information on the symptoms typical of Coronavirus and on the recent movements of each individual are the responsibility of healthcare professionals and the civil protection system, which are the entities tasked with ensuring compliance with the public health rules that were recently adopted in Italy; and – employers must refrain from collecting information on the presence of any flu like symptoms of the employee and their close workcontacts or those contacts outside of work. <p>The IDPA remarked that:</p> <ul style="list-style-type: none"> – the obligation on the employee to inform the employer of any danger to health and safety at the workplace is left unprejudiced; – the employer may invite their employees to make, where necessary, such communications by facilitating the way they are routed, including through dedicated channels; – the obligations for the employer to inform the competent entities of any change in the 'biological' risk to health at work arising from the Coronavirus are left unprejudiced along with 	2 March 2020	IDPA's press release Link



Development	Summary	Date	Links
	<p>the other tasks related to health surveillance of workers through the competent doctor, such as the possibility to have the most exposed workers undergo a medical visit.</p> <p>Where an employee performing duties that entail contact with the public (e.g. at a front office, at a service desk) encounters a suspected Coronavirus case in the course of their work, that employee will ensure that the competent health services are informed - including through the employer - and will follow the preventive instructions provided by the healthcare professionals consulted.</p>		
Emergency provisions to contrast COVID-19 with data protection relevance	<p>On 22 March 2020 a Decree of the Italian Head of Government was issued which suspended various kinds of activities.</p> <p>The Decree specifically included a: "Protocol to regulate measures to contrast and contain COVID-19 at workplaces", which was signed by the representative organisations of employers and employees on 14 March 2020, making it legally binding for undertakings whose activities have not been suspended. The Protocol contains guidelines to help undertakings adopt anti-contagion security measures, allowing the continuation of work in a safer context. The Protocol allows for access to premises to be on the condition of checking employees/providers/other subjects' body temperature and to collect, if absolutely necessary, declarations on contacts and movements to identify possible contamination risks. The Protocol, points to data protection principles to be considered, information obligations, the legal basis for the data processing and other data protection requirements.</p> <p>This Protocol can be further implemented locally after appropriate negotiations with the unions.</p>	22 March 2020	<p>Decree of the Italian Head of Government of 22 March 2020 (only available in Italian language)</p> <p>Link</p> <p>Protocol to regulate measures to contrast and contain Coronavirus outbreak at workplaces, signed on 14 March 2020 (only available in Italian language)</p> <p>Link</p>
IDPA's communication on pending proceedings	<p>The IDPA has communicated the suspension of the administrative proceedings pending before the IDPA until 15 April 2020 due to COVID-19. This measure may undergo changes due to legislative developments.</p>	28 March 2020	<p>IDPA's communication on pending proceedings (only available in Italian language)</p> <p>Link</p>



Development	Summary	Date	Links
IDPA's publishes press release on data protection implications of remote teaching during to COVID-19	<p>The IDPA issued a press release relating to measures addressing schools, universities and families and providing indications on data protection implications of remote teaching due to COVID-19.</p> <p>The IDPA remarked that schools and universities adopting remote teaching systems do not need data subjects' consent because they are processing personal data as a result of their official tasks under the law.</p> <p>In choosing remote teaching systems, schools and universities should comply with the privacy-by-design and privacy-by-default principles under the GDPR.</p> <p>IDPA also provided guidance on the provider's role and referenced the application of the GDPR's principles (purpose limitation, fairness and transparency), taking into account possible employment implications.</p>	30 March 2020	<p>IDPA's press release making available the measure addressing schools, universities and families and providing indications on data protection implications of the remote teaching due to COVID-19 (only available in Italian language).</p> <p>Link</p> <p>IDPA's measure n. 64 of 26 March 2020 providing indications on data protection implications of the remote teaching due to COVID-19.</p> <p>Link</p>



Lithuania

Contributors



Rintis Puisys
Partner

T: +370 5 239 2391
rimtis.puisys@
eversheds.lt



Akvilė Jurkaitytė
Associate

T: +370 5 239 2391
akvile.jurkaityte@
eversheds.lt

Development	Summary	Date	Links
Data protection in the context of COVID-19	<p>On 19 March 2020, The European Data Protection Board updated its notice on data processing regarding COVID-19. On the same day, additional information was provided by the Lithuanian State Data Protection Inspectorate ("SDPI"). This considered the following questions:</p> <p><u>Can personal data related to COVID-19 be processed?</u></p> <p>The issue of processing COVID-19-related personal data becomes particularly relevant as the virus spreads and states respond to the situation. While the processing of such data is not in itself prohibited, controllers must consider and maintain a balance between their own interests, those of third parties, and data subjects, and implement the requirements and measures set forth in the GDPR.</p> <p><u>What COVID-19 related data can be processed?</u></p> <p>As with the processing of other personal data, the principle of data minimisation applies. In terms of the processing of personal health data, in this case, the requirements for the processing of special categories of data must also be ensured.</p> <p>Subject to the above principles and requirements, controllers may (and in some cases must, subject to employment law) process data relating to:</p> <ol style="list-style-type: none"> 1) whether the person was traveling to a "country of risk"; 	19 March 2020	<p>SDPI notice (in Lithuanian)</p> <p>Link</p>



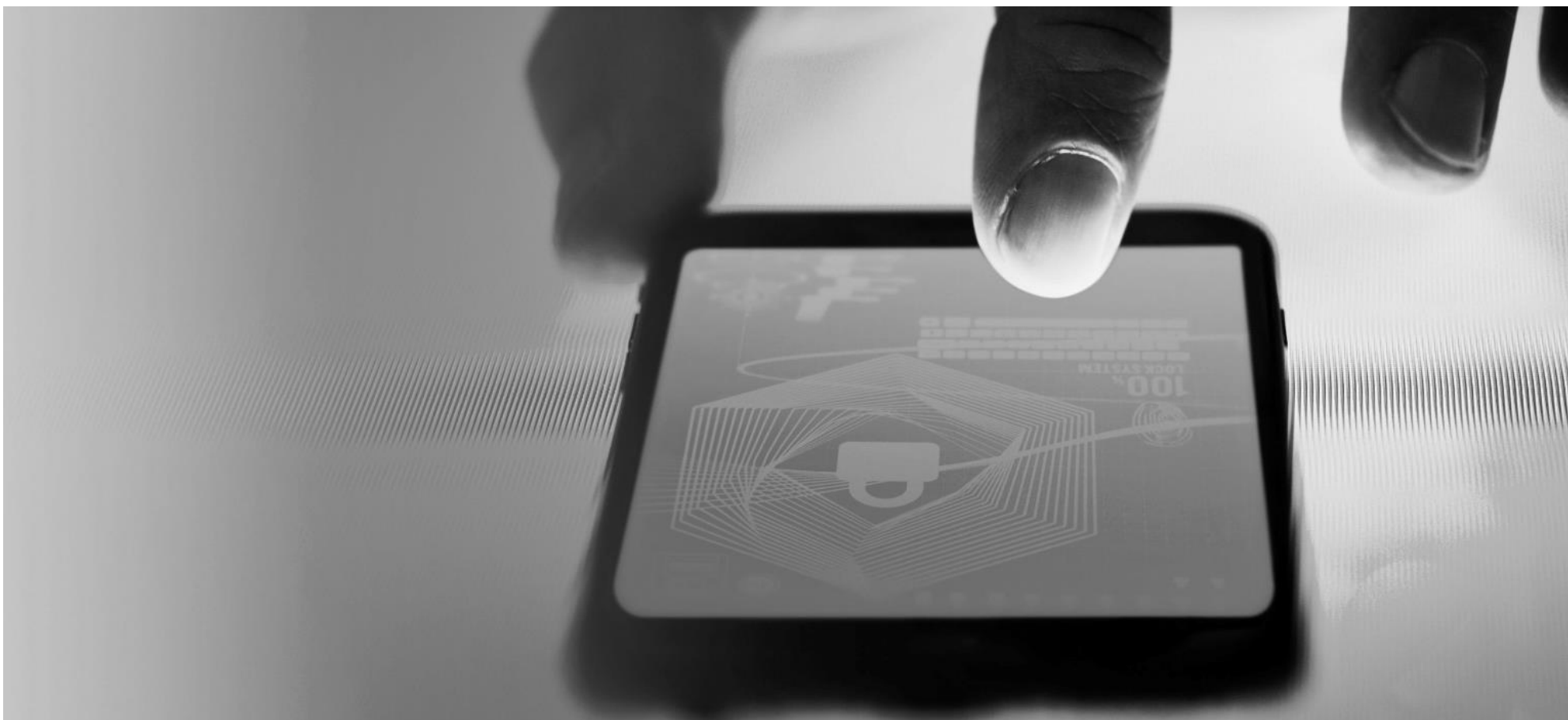
Development	Summary	Date	Links
	<ol style="list-style-type: none"> 2) whether the person was in contact with a person travelling to a “country of risk” or with a person sick with the COVID-19; 3) whether or not the person is present at home due to quarantine (without giving a reason) and quarantine period; and 4) whether the person is ill (without specifying a specific disease or cause). <p>Controllers can obtain this information:</p> <ol style="list-style-type: none"> 1) whether data subjects (staff, visitors) have symptoms of the Covid-19 virus; or 2) whether they are diagnosed with COVID-19. <p>The position of the SDPI is that in the case of this latter personal data, controllers have no right to document the received information or data files. In practice, it is conceivable that there will be some cases where the employer will inevitably retain such data for a period of time (e.g. as evidence of additional protection measures), however, the implementation of data minimisation and other GDPR principles and requirements should be ensured. Controllers (here employers) will also be able to process personal data relating to changed circumstances, such as remote work, flexible work schedules and so on.</p> <p><u>What kind of data processing is not allowed?</u></p> <p>Although the processing of certain data relating to COVID-19 and the receipt of related information is not prohibited, controllers must in any case assess the scope of the data processed.</p> <p>In this respect, it is important to remember that the processing of surplus or unrelated data will not be compatible with GDPR requirements.</p> <p>Taking into account, among other things, the position of the SDPI, the requirements of the GDPR are incompatible with:</p> <ol style="list-style-type: none"> 1) collection and processing of medical certificates; 		



Development	Summary	Date	Links
	<ol style="list-style-type: none"> 2) processing of personal temperature readings or other evidence of illness; 3) processing of other data, unless such data is necessary for the implementation of state or company-specific COVID-19 prevention measures (excessive processing of employee control, monitoring, other data); and 4) providing data to third parties in the absence of such a basis for processing (e.g. transfers to group companies, transfers of non-personal data used solely for statistical purposes, etc.). <p>As a general rule, informing other employees of a specific person identified as having COVID-19 in a company or organisation will not be compatible with GDPR requirements. In this case, only general information on the detection of COVID-19 and appropriate preventive measures are generally permitted. Additional, specific information (about increased risks, measures to be taken, etc.) may be provided to employees who have been, or may have been, “contact persons”, but even in this case, such additional information must be aimed at preventing the identification of person identified as COVID-19 case.</p> <p><u>What measures should controllers implement?</u></p> <p>As with other processing of personal data, controllers are required to implement the technical and organizational measures provided for in the GDPR in relation to the processing of the personal data in question, in particular</p> <ol style="list-style-type: none"> 1) the definition of the scope of the data processed, the purposes of the processing and the legal basis. Personal data will normally be processed for risk management purposes related to COVID-19; 2) establishment of a data retention period. The legislation does not specify a specific time limit within which companies/organisations must or may process data relating to COVID-19, and this term shall be set by the controller, taking into account the specific data and its relevance (e.g. quarantine period, remote work period and etc.); 		



Development	Summary	Date	Links
	3) ensuring adequate data security, including control of access to the data being processed;		
	4) informing data subjects of the processing of the personal data in question; and		
	5) where appropriate, the performance of data subject impact assessments.		





Contributors

Malaysia



Suaran Singh Sidhu

Partner

T: +603 9212 9287

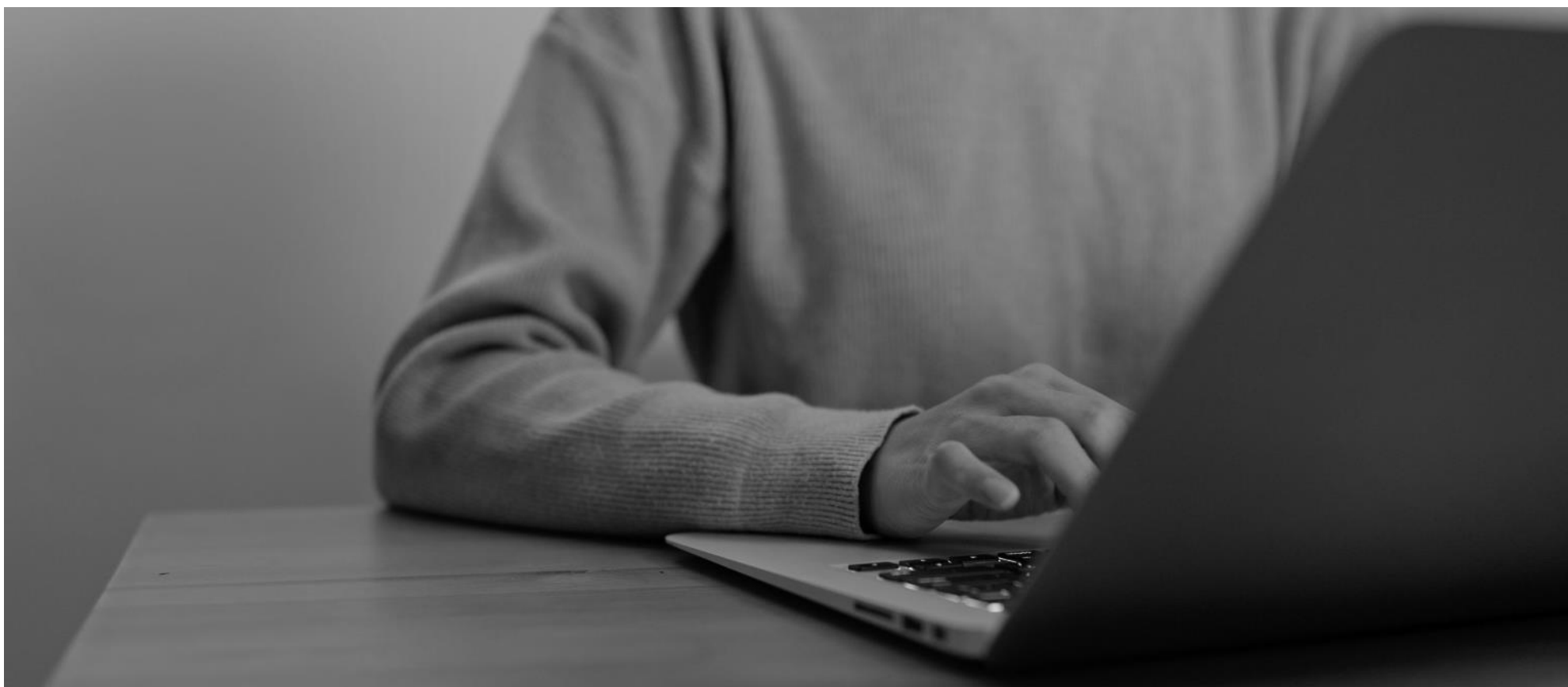
suaransidhu@

law-partnership.com

Development	Summary	Date	Links
MCMC and the Royal Malaysia Police Crack Down on the Spread of Fake News on COVID-19 Outbreak	<p>In a joint effort to curb the spreading of false and/or unverified information online, MCMC and the Royal Malaysia Police have reported the detention of four (4) individuals as of 29 January 2020 for purportedly spreading false information on the Novel Coronavirus outbreak on their respective social media accounts.</p> <p>The detainees are to be investigated under Section 233 of the Communications and Multimedia Act (CMA) 1998, which provides for a maximum fine of RM50,000, or imprisonment for up to a year, or both, and a further fine of RM 1,000 for every day during which the offence is continued after conviction.</p>	29 January 2020	<p>Press Release by MCMC</p> <p>Link</p>
CyberSecurity Malaysia's Recommendations and Best Practices Guide on Working From Home in Light of the COVID-19 Outbreak	<p>CyberSecurity Malaysia, an agency under the MCMC, has released its recommendations and best practices on working from home ("the Release").</p> <p>This Release follows the Movement Control Order ("MCO") declared by the Prime Minister's Office, which aims to control the spread of COVID-19 and will be in place from 18th March 2020 until 14th April 2020, as at the time of writing.</p> <p>As a result of the MCO, many governmental and private organisations have commenced "work from home" schemes, and the Release aims to recommend measures that may be taken by network providers, organisations, and the general public in order to mitigate the risks of cyberattacks.</p> <p>The measures and best practices recommended by CyberSecurity Malaysia include warning the public against phishing attempts and recommending that organisations ensure all systems, networks (including virtual private networks (VPNs)), and</p>	21 March 2020	<p>Press Release</p> <p>(Language: Malay – this press release was not translated into the English language)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>devices used are updated with the latest “patch” changes, especially to fix security vulnerabilities.</p> <p>The Release further provides the public with various channels to report incidents of cybersecurity breaches, including a 24-hour hotline and a “Cyber999” application available for download on the Apple App Store or Google Play Store.</p>		





Netherlands

Contributors



Marijn Rooke
Associate

T: + 31 1 02 48 80 62
marijnrooke@
eversheds-sutherland.nl



Robbert Santifort
Associate

T: +31 6 81880472
robbertsantifort@
eversheds-sutherland.com



Olaf Van Haperen
Partner

T: +31 1 02 48 80 58
olafvanhaperen@
eversheds-sutherland.nl



Sarah Zadeh
Associate

T: +31 1 02 48 82 66
sarahzadeh@
eversheds-sutherland.com

Development	Summary	Date	Links
The Dutch Data Protection Authority published tips for working remotely	<p>The Dutch Data Protection Authority has published a few safety tips for working remotely during the COVID-19 crisis:</p> <ol style="list-style-type: none"> 1. <u>Work in a secure environment</u> If possible, only work in a secure home working environment. For example, try to log in at home using your organisation's server, so that you'll see the same screen as when you are in the office. If possible, use the equipment (laptop or tablet, for example) provided by your organisation. 2. <u>Protect sensitive documents</u> If there are sensitive documents that are not on the server, but only on a USB-stick or on paper, make sure they are saved onto the organisation's server. 3. <u>Be careful with the use of (video) chat services</u> For conversations in which sensitive data is discussed, it is preferable to use the available secure means of communication, such as regular telephone calls. Sometimes organisations have secure options for video calling or chatting. 4. <u>Watch out for phishing emails</u> 	18 March 2020	<p>The Dutch Data Protection Authority published tips for working remotely (in Dutch only)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>If you receive an e-mail from an unknown sender, do not click on links in these emails, do not open attachments and do not fill in any details.</p> <p>Cyber criminals are exploiting the COVID-19 crisis by sending phishing emails. These are fake e-mails with, for example, information about COVID-19. These criminals try to extract information or install malware on your computer.</p>		
Dutch Data Protection Authority gives organizations more time due to the COVID-19 crisis	<p>The Dutch Data Protection Authority stated that, during the COVID-19 crisis, organisations are given more time to respond to questions of the Dutch Data Protection Authority. Deadlines for providing information to the regulator will be extended where necessary.</p> <p>Furthermore, the Dutch Data Protection Authority will clear the way for initiatives to protect public health. By doing so, the Dutch Data Protection Authority wishes to give organisations time to focus their full attention to combating the consequences of the COVID-19 crisis.</p>	20 March 2020	<p>Dutch Data Protection Authority gives organizations more time due to the COVID-19 crisis (in Dutch only)</p> <p>Link</p>
Dutch Data Protection Authority states that access to medical records is only permitted with the patient's consent	<p>In a letter to the Minister of Medical Care, the Dutch Data Protection Authority stated that doctors at the general practitioner's post or emergency room may only access their GP's medical records via an electronic exchange system with the consent of COVID-19 patients. Those who have not yet given permission can do so on the spot. In this case, this may also be done verbally. Access without permission is only permitted if a patient is unable to give such permission.</p> <p>The Dutch Data Protection Authority understands the desire to soften the rules regarding the processing of medical data related to COVID-19 patients. However, the Dutch Data Protection Authority points out that patients' privacy must also be respected during times of crisis.</p>	30 March 2020	<p>Dutch Data Protection Authority states that access to medical records is only permitted with the patient's consent (in Dutch only)</p> <p>Link</p>
Using telecom data to curb the spread of COVID-19 is only possible if there a specific legislation that regulates such use	<p>The Dutch Data Protection Authority stated that using location data may help the government to curb the spread of COVID-19, but that location data may only be used as such if there is specific legislation that regulates the use of location data for such</p>	1 April	<p>Using telecom data to curb the spread of COVID-19 is only possible if there a specific</p>



Development	Summary	Date	Links
	<p>purposes. In the view of the Dutch Data Protection Authority that location data is not anonymous data.</p> <p>Furthermore, the Dutch Data Protection Authority stated that if an emergency act was passed to regulate the use of location data by the government, specific safeguards must be put in place.</p>		<p>legislation that regulates such use (in Dutch only)</p> <p>Link</p>
<p>Dutch Data Protection Authority states that, despite COVID-19, employers are not allowed to process medical data of their employees</p>	<p>The Dutch Data Protection Authority stated that, despite the current COVID-19 crisis, employers are not allowed to process medical data of their employees. Therefore, employers may not ask their employees about their health or keep records of sickness reports.</p> <p>Employers are <u>not</u> allowed to test employees themselves. Employers are only allowed to have a (company) doctor test their employees for COVID-19-related symptoms or ask the employee to monitor their own health closely.</p> <p>However, when an employee shows signs of a cold or the flu, it may send the employee home under the 'special circumstances' of the COVID-19 crisis. Employers are advised to follow any instructions from the National Institute for Public Health and the Environment ('RIVM') and local Joint Health Services.</p>	N/A	<p>Dutch Data Protection Authority states that, despite COVID-19, employers are not allowed to process medical data of their employees (in Dutch only)</p> <p>Link</p>



Poland

Contributors



Marta Gadomska-Golab
Partner

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



Aleksandra Kunkiel-Kryńska
Partner

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



Agnieszka Sagan-Jezowska
Senior Associate

T: +48 22 50 50 730
agnieszka.sagan-jezowska@
eversheds-sutherland.pl

Development	Summary	Date	Links
Polish Labour Inspectorate publish the statement on obtaining the additional information from the employees for COVID-19 prevention	The Polish Labour Inspectorate (“ PIP ”) published a statement on obtaining additional information from employees for COVID-19 prevention. PIP presents the labour measures and limitations regarding measuring body temperature, requesting travel information or ordering additional medical tests. The statement of PIP is more restrictive in relation to obtaining additional information from employees than the DP Authority or EDPB statements.	26 February 2020	Statement of PIP Link
Data Protection Authority’s statement on processing the personal data on COVID-19 prevention	Under the Polish Data Protection Authority’s (“ PUODO’s ”) statement, GDPR should not be used as an obstacle to the implementation of activities in connection with COVID-19 prevention. In the statement, the PUODO said that there is a legal basis of processing the additional personal data, including medical information, under the GDPR. The PUODO emphasised that the processing of personal data should meet the general rules of the GDPR, in particular the minimisation rule. PUODO’s statement aligns with the statement of the President of the European Data Protection Board.	12 March 2020	Statement of PUODO Link



Russian Federation

Contributors



Victoria Goldman
Managing Partner

T: +7 812 363 3377
victoria.goldman@
eversheds-sutherland.ru



Ekaterina Mironova
Principal Associate

T: +7 495 662 6434
ekaterina.mironova@
eversheds-sutherland.ru



Ivan Kaisarov
Senior Associate

T: +7 812 363 3377
ivan.kaisarov@
eversheds-sutherland.ru

Development	Summary	Date	Links
Use of thermal imagers during the COVID-19 epidemic - new clarifications	<p>Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor") has issued clarification on the use of thermal imagers by employers.</p> <p>Measuring body temperature without the individual's consent is allowed only if carried out with a legal basis in labor legislation. The employer, as a rule, is not entitled to request information about employees' health status. The exception provided by law is when such health data may give an indication of the employee's capacity to perform their work functions. Since measuring temperature to detect the virus in employees gives a strong indication as to the employee's capacity to continue performing their work functions, it is not required to obtain consent from the employee to measure their temperature in the current situation.</p> <p>Visitors to company property who do not have an employment relationship with the company are expressing their consent to their temperature being measured (though in an anonymous way) by showing intent to visit company premises.</p> <p>Employees, as well as visitors, must be duly notified that they will be subject to temperature measurements. We recommended placing a written announcement to that effect at the entrance to the company's premises.</p> <p>Roskomnadzor also recommends erasing the results of the temperature measurement (thermal image) within 24 hours after it has been collected.</p>	10 March 2020	<p>Clarifications on the official website of the Roskomnadzor</p> <p>Link</p>



Singapore

Contributors



KK Lim

Head, Cybersecurity, Privacy and Data Protection

T: +65 6361 9307

kklim@

eversheds-harryelias.com



Janice Lee

Foreign Legal Associate

T: + 65 6361 9821

janicelee@

eversheds-harryelias.com



Valencia Soh

Associate

T: + 65 6361 9829

ValenciaSoh@

eversheds-harryelias.com

Development	Summary	Date	Links
Advisory on Collection of Personal Data for COVID-19 Contact Tracing	The PDPC issued an advisory on the collection, use and disclosure of personal data of visitors of organisations (including visitors' national identification numbers) for COVID-19 contact tracing and other response measures in the event of an emergency.	13 February 2020	PDPC Advisory Link



Spain

Contributors



Juan Díaz
Managing Partner

T: +34 91 429 43 33
jdiaz@
eversheds.es



Vincente Arias Máiz
Partner

T: +34 91 429 43 33
varias@
eversheds.es



Celia Bouzas González
Senior Associate

T: 34 91 429 43 33
cbouzas@
eversheds-sutherland.es

Development	Summary	Date	Links
The Spanish Data Protection Agency issues a legal report regarding employers' legitimation to process employee data in prevention of COVID-19 pandemic	<p>The Spanish Data Protection Agency ("AEPD") has issued a legal report clarifying how GDPR applies to processing data in the framework of preventing the spread of the COVID-19 pandemic and, specifically, establishing public authorities' and employers' legitimation for processing.</p> <p>With regards to companies, the report clearly establishes that employers are entitled to process employee health data (for instance, employee temperature checks or reporting of other COVID-19 symptoms), as well as other data which it may rationally use for preventing the spread of the pandemic (for instance, information on the places where the employee has stayed outside work), and that it does so on the basis of a double legitimation:</p> <ul style="list-style-type: none"> – Firstly, employers are entitled in compliance with a legal obligation (Article 6.1.c of GDPR) and for performing a task in the public interest (Article 6.1.e of GDPR) in connection with employers' obligation to care for the health of employees, as set out in section 14 of the Spanish Health and Safety Act. – Additionally, employers are entitled, insofar as the processing is necessary, to protect the vital interests of the data subject 	13 March 2020	<p>AEPD report</p> <p>Link</p>



Development	Summary	Date	Links
	<p>or of another natural person (its employees in general) according to Article 6.1.d of GDPR. This, again, covers health data (Article 9.2.c of GDPR). Though legitimised to process data, employers still need to comply with the rest of their obligations under both GDPR (including, for example, transparency and security) and employee health and safety laws.</p>		
The AEPD issues a notice on COVID-19 Self-Assessment Apps and Websites	<p>If Spanish citizens use applications or websites to self assess their symptoms that are not owned by public authorities but are offered by private entities or persons, the legal basis of processing of public interest, or guaranteeing the vital interests of those affected or of third parties will not apply. In this case, the AEPD recommends that citizens are particularly careful when it comes to finding out who is going to process their personal data, for what purpose and with what guarantees.</p> <p>There is also a provision that all citizens who have tested positive for COVID-19 can be geolocated via the mobile phone that they have previously provided so that they can be monitored. The AEPD has stated that it must start from the broad powers that the health authorities have in exceptional situations (such as COVID-19), taking into account that one of the exceptional measures for managing the health crisis situation caused by COVID-19 is to limit the freedom of movement of people. However, the only information that should be provided to telecommunications operators for the purposes of geolocation, if any, would be the mobile phone number to be geolocated, unless the Ministry of Health considered that it was essential to provide some other information for the purposes of monitoring the disease.</p>	26 March 2020	AEPD Notice Link



Contributors

Sweden



Josefine Karlsson
Associate

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



Torbjörn Lindmark
Partner

T: +46 8 54 53 22 27
torbjornlindmark @
eversheds-sutherland.com

Development	Summary	Date	Links
Guidelines published on data processing during the COVID-19 crisis	<p>The Swedish Data Protection Authority (“DPA”) has published brief guidelines on the processing of personal data during the COVID-19 crisis.</p> <p>The information is mainly aimed for employers and clarifies that information relating to an individual infected by COVID-19 is deemed to be health information and therefore classified as special category of personal data. It is also likely that information that an individual has been placed in quarantine under disease control laws is considered to be health information too. However, the following is not deemed to be health information: (i) information on an individual returning from a risk zone; and (ii) information on an individual being under voluntary quarantine (as long as no further information is provided).</p> <p>Employers may process this personal data about their employees provided that it is strictly necessary under Article 9(b) GDPR. The DPA reminds employers that the general principles for data processing must still be met, that personal data must only be processed when necessary and to only allow access to the data on a need to know basis.</p> <p>The DPA also clarifies that contact information of employees and their next of kin may be processed by employers if this is based on a legitimate interest, since it is usually in the interest of both parties that the employer can get in contact in case of a workplace accident or sickness at work.</p> <p>Furthermore, the DPA has also provided a Q&A which considers questions such as whether or not an employer can inform its employees if an employee has been infected, or if temperature controls can be made at work.</p>	13 March 2020	<p>Information and Q&A (in Swedish)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>Along with advice for employers, the DPA also considers other types of information, for example in relation to live video meetings between doctors and patients. The DPA states that such meetings can be held provided that adequate security measures are taken by the caretaker and any data processors. Reference is made to regulations issued by the National Board of Health and Welfare, where it is stipulated that certain security measures must be taken when patient data is processed, including on the internet. For example, it is a requirement that patient data is protected from unauthorized access by way of encryption and secure log in.</p>		





Contributors

Switzerland



Michel Verde

Senior Associate, Attorney-at-Law

T: +41 44 204 90 90
michel.verde@
eversheds-sutherland.ch

Development	Summary	Date	Links
Processing of employees' personal data in the context of the COVID-19 situation	<p>The Swiss data protection authority (the Federal Data Protection and Information Commissioner) published guidance for data processing in connection with COVID-19, which is also relevant for employers processing personal data about their employees due to COVID-19 situation. The data protection law also applies to the processing of personal data in connection with COVID-19. The general principles of Swiss data protection law must therefore be observed.</p> <p>Health related information about whether an individual has been infected with COVID-19 or exhibits symptoms of a COVID-19 infection are so-called sensitive personal data and are part of the individual's intimate sphere. However, under certain conditions, it is lawful (and even necessary) for an employer to process such COVID-19 related personal data:</p> <p>First of all, the processing of the personal data has to be purpose related and proportionate. This means in particular that the processing of the personal data has to be necessary and suitable to prevent infection of employees (or clients or other individuals) at work. The employer is therefore, for example, allowed to be informed if an employee has been infected with COVID-19 or exhibits symptoms of such infection or if he/she has been in close contact with an individual that exhibits symptoms of an infection, so that the employer can implement the necessary measures to safeguard the health of the other employees. Whenever possible, such Information should be collected from the concerned employee him-/herself. Due to his/her duty of loyalty, an employee is obliged to inform the employer about a possible infection with COVID-19. On the other hand, an employer would not be allowed to conduct detailed health check of the employees</p>	1 April 2020	Federal Data Protection and Information Commissioner guidance Link



Development	Summary	Date	Links
	<p>by asking them to fill out a health status questionnaire before entering the company's premises.</p> <p>Secondly, information about a (possible) COVID-19 infection of an employee has to be kept confidential. They may only be shared with those persons who really need the information. This is usually the case for HR and often also for the supervisor. With regard to other employees in the company who were in touch with the affected employee and may therefore have been infected too, it is normally sufficient to simply inform them that they have been exposed to a risk of COVID-19 infection and that they must take appropriate precautions (e.g. observe whether they develop symptoms of a COVID-19 infection, self-isolation, etc.); a disclosure of the name of the affected colleague will not be justified. Similarly, the disclosure of non-anonymised Information about COVID-19 infections to other group entities for resource planning purposes will normally not be lawful due to lack of necessity. Also, the COVID-19 related personal data may only be retained as long as necessary and must be deleted as soon as the risk of COVID-19 infections at work does not exist any longer or as soon as the corona virus situation ended.</p> <p>Thirdly, the employer must inform the employees about how the COVID-19 related personal data will be handled. This includes in particular information on the purpose of the processing, the recipients of the information and the retention period.</p>		



United Kingdom

Contributors



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



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

Development	Summary	Date	Links
UK Parliament publishes Coronavirus Bill	<p>The UK Parliament has published the Coronavirus Bill, which amends existing legislative provisions and introduces new statutory powers aimed at mitigating the impact of the COVID-19 outbreak in the UK. The Bill contains several provisions on data protection.</p> <p>In particular, the Bill provides that personal data may not be used or disclosed if the use or disclosure would contravene the Data Protection Act 2018. In determining use or disclosure, S 27 (1) and (2) provide for anonymised information or where disclosure is in accordance with the terms on which the information was disclosed to that person. The Bill also provides for an extension of retention periods for fingerprints and DNA profiles.</p> <p>The Bill will expire at the end of a period of 2 years, with a review every six months.</p>	24 March 2020	<p>Bill</p> <p>Link</p>
ICO publishes a blog post on community groups and COVID-19	<p>The Information Commissioner's Office ("ICO's") Director of Regulatory Assurance has published a blog entry providing guidance for community groups on handling personal data during the COVID-19 pandemic.</p> <p>The blog provides guidance to community groups (including church groups and neighbourhood and resident associations supporting the work of existing community groups, services and charities) on the key data protection principles to consider when using and sharing personal data in the context of their activities during the COVID-19 crisis.</p> <p>In particular, the blog emphasises the importance of:</p> <ul style="list-style-type: none"> – Transparency – being clear, open and honest with people about what you are doing with their personal information, and how to use privacy notices effectively to communicate information; 	26 March 2020	<p>ICO Blog Post</p> <p>Link</p>



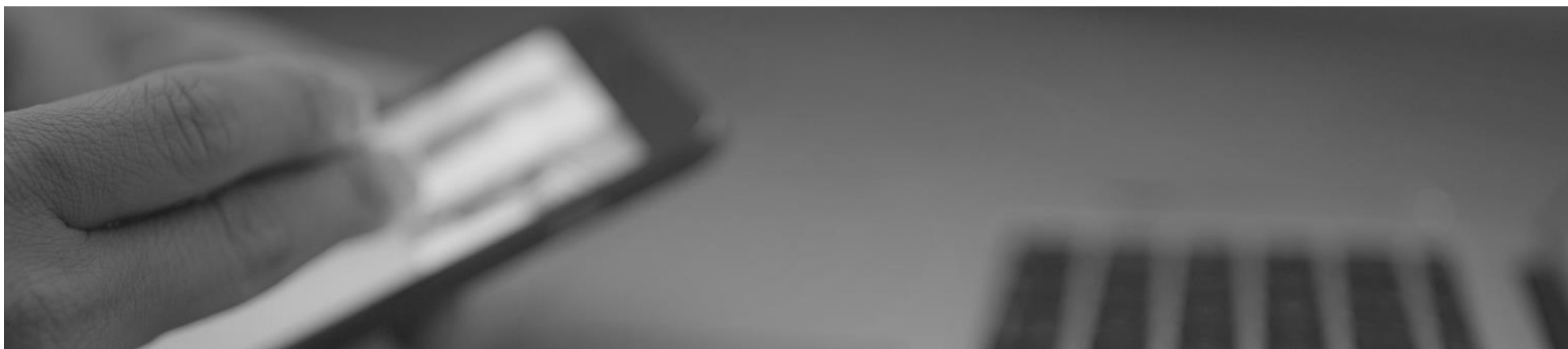
Development	Summary	Date	Links
	<ul style="list-style-type: none"> – Sharing personal data – data should be shared when required in emergencies and, to the extent possible, thinking ahead about what information is likely to be shared and how that can be carried out securely. – Using personal data lawfully – in particular, groups should consider whether: the person expect me to use their information in this way (legitimate interests); the person has given their clear and unambiguous consent to the use of their personal information (consent); and/or the person's health or safety is at risk if their personal data isn't used in a particular way (vital interests). – Special rules around special category personal data – in particular, groups should consider whether: the information is required to protect a person at risk (safeguarding individuals); the person has given their explicit consent to use the information (consent); and/or the information could save someone's life (vital interests). – Security – the ICO has produced some specific security tips for community groups. – Data minimisation – only using the personal data needed to help vulnerable people during the COVID-19 crisis and to securely delete or destroy the information when it is no longer needed. – Recording activities – recording the decisions made involving the use of personal information. 		
ICO discusses use of mobile phone tracking data to help fight coronavirus does not breach privacy laws	<p>The ICO released a statement confirming that the use of generalised mobile phone location data in the fight against coronavirus does not breach privacy laws where the data is properly anonymised and aggregated – it does not fall under the scope of data protection law because no individual can be identified from it.</p> <p>The ICO continues by assuring readers that the safety and security of the public remains its primary concern and that it will continue to work alongside the government to provide advice about the application of data protection law during the COVID-19 outbreak.</p>	28 March 2020	ICO Statement Link



Development	Summary	Date	Links
Government announces new health data platform to facilitate decision making	<p>The Government published a blog post relating to the launch of a new health data store – collating multiple data sources into a single secure location – to enable national organisations responsible for coordinating the response to access “secure, reliable and timely data” in order to make informed, effective decisions in the COVID-19 crisis.</p> <p>The data will come from across the NHS and social care and from partner organisations. It will include data such as 111 online/call centre data from NHS Digital and Covid-19 test result data from Public Health England. The data will then be integrated and cleansed to develop a single database, under NHS England and NHS Improvement’s control.</p> <p>The data will be presented as dashboards providing a live view of the metrics needed to track and understand the current spread of the crisis, and the capacity in the healthcare system to deal with it. The Government aims to make as much data openly available as possible over time, including a separate dashboard to support public understanding. It will make the code and the data open source where possible.</p> <p>The Government states that once the public health emergency situation has ended, data will either be destroyed or returned in line with the law and the strict contractual agreements that are in place between the NHS and partners.</p> <p>In developing the new database, the Government has enlisted the help of firms from across the technology sector, including: NHSX, Microsoft, Palantir Technologies UK, Amazon Web Services, Faculty and Google.</p>	28 March 2020	Government blog post Link
ICO launches coronavirus hub	The ICO launched a new information hub to help individuals and organisations navigate data protection law compliance and rights during the COVID-19 pandemic. The ICO will add new information to the hub as and when it is produced, during the continuation of the pandemic.	30 March 2020	ICO coronavirus hub Link
First-Tier Tribunal (information Rights) issues stay of all DPA, FOIA and EIR	The First-Tier Tribunal General Regulatory Chamber (information Rights) has issued a general stay of all proceedings under section 48 of the Data Protection Act 1998, section 162 of the DPA 2018 and section 57 of the Freedom of Information Act 2000 (including	1 April 2020	FTT Notice Link



Development	Summary	Date	Links
proceedings in light of coronavirus pandemic	<p>proceedings under that section as modified under regulation 18 of the Environmental Information Regulations 2004) for a period of 28 days, and all time limits in any new and current proceedings are extended by the same period.</p> <p>The stay does not apply to cases with specific directions issued on or after 1 April, and Parties may apply to the Tribunal, with reasons and on notice to the Information Commissioner, for the Directions to be amended, suspended or set aside or for further Directions in relation to those proceedings.</p>		
UK Government issues notifications to companies to share information during the Coronavirus pandemic	<p>Four notices have been issued from the Department of Health and Social Care (“DHSC”) which require organisations providing health services, GPs, local authorities and arm’s length bodies of the DHSC to share data during the coronavirus pandemic. The notices make clear that this data sharing (which will include confidential patient data) is required to support the Government’s response to the virus. The processing of this data is permitted under the notices where it is for a “Covid-19 Purpose”. Such purposes include identifying potential patients, treating those currently infected, delivering services connected with health and social care, conducting analysis, research and monitoring.</p>	1 April 2020	<p>UK Government statement</p> <p>Link</p>





United States

Contributors



Alexander Sand
Associate

T: +1.512.721.2721
alexanderf.l.sand@
eversheds-sutherland.com



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



Pooja Kohli
Litigation Specialist

T: +1.212.389.5037
pkohli@
eversheds-sutherland.us



Sarah Paul
Partner

T: +1.212.301.6587
sarahpaul@
eversheds-sutherland.com

Development	Summary	Date	Links
Safety measures to consider in light of COVID-19	<p>General counsel and cyber security teams are focussing on their company's COVID-19 safety measures in order to protect against hackers. Legal and IT departments should ensure employees are reminded of at least two critical things they should do in this heightened risk environment:</p> <ul style="list-style-type: none"> – Be wary of clicking on links embedded in emails and entering in credentials. – Ensure proper remote access, as accessing company servers without using a secure connection exposes servers to hackers. <p>Five quick and critical, yet inexpensive, questions to ask in order to help ensure your company remains well positioned to successfully respond to cyber-attacks are as follows:</p> <ol style="list-style-type: none"> 1. Ensure the response plan does not reside solely on company servers. In case of a cyber-attack, accessing documents 	10 March 2020	<p>Eversheds Sutherland article</p> <p>Link</p>



Development	Summary	Date	Links
	<p>electronically may not be an option. Ensure you print out your response plan and maintain it in hard copy.</p> <ol style="list-style-type: none">2. If you do print your response plan, check whether the response team has copies of the plan at home. It is important to store hard copies of these critical documents safely at home.3. Confirm that the call roster for key response team members (both internal and external) includes work, cell and other contact numbers. This should not just be stored electronically.4. Confirm that you have a good sense of your regulatory and contractual notification obligations in the event of a breach.5. Check to see when cyber insurance was last reviewed, that it is current and that it covers what you want it to cover. It is important that you are covered for the latest threats and types of attacks.		



General Updates



General EU and International

Contributors



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



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

Development	Summary	Date	Links
EDPS released its Preliminary Opinion on data protection and scientific research	<p>The European Data Protection Supervisor (“EDPS”) published its initial opinion on data protection and scientific research (the “Preliminary Opinion”). The Preliminary Opinion explores the implications of GDPR in the sphere of scientific research which, by its nature, involves the exchange of information and the generation, evaluation and digitisation of personal data. Data resulting from scientific research is incredibly valuable to hold corporate giants to account, and data protection obligations should not act as an excuse for powerful market players to evade accountability and transparency.</p> <p>In the Preliminary Opinion, EDPS recommends escalating the communication between data protection authorities and ethical review boards in order for a common understanding to be reached as to what constitutes ‘genuine’ scientific research, and for EU research programme frameworks and data protection standards to become more closely aligned.</p>	6 January 2020	Preliminary Opinion Link
EU Commission task force hopeful for UK adequacy by the end of 2020	<p>According to the European Commission <i>ad hoc</i> working party on Article 50 (UK Brexit) UK adequacy for data transfers could be resolved by the end of 2020 if certain requirements are fulfilled.</p> <p>The Task Force for Relations with the UK has held internal preparatory discussions on the future relationship with the UK on the protection of personal data and cooperation and equivalence in financial services.</p> <p>Internal slides state that if the UK leave the EU with an agreement on 31 January 2020, there will be a transition period of 11 months during which time an adequacy decision may be</p>	10 January 2020	Copy of Internal Slides Link



Development	Summary	Date	Links
	negotiated. The task force suggests that the UK's future data protection framework could include an adequacy decision under the GDPR as well as recognising existing adequacy decisions, using Binding Corporate Rules and Standard Contractual Clauses.		
CJEU publishes AG opinion on the applicability of the ePrivacy Directive to national security and counter-terrorism activities	<p>The Court of Justice of the European Union ("CJEU") has published Advocate General ("AG") Manuel Campos Sánchez-Bordona's opinions on the Privacy International case (C-623/17), the joined cases of La Quadrature du Net and Others (C-511/18) and French Data Network and Others (C-512/18) and the case of Ordre des barreaux francophones et germanophone and Others (C-520/18). Collectively, the cases consider the application of the Directive on Privacy and Electronic Communications (the "ePrivacy Directive") to national security activities and activities aimed at combatting terrorism.</p> <p>The AG stated that the ePrivacy Directive does not apply to activities carried out by public authorities on their own account which aim to safeguard national security. The AG noted that the ePrivacy Directive will, in principle, be applicable where providers of electronic services are required by law to retain data belonging to their subscribers and to allow public authorities to have access to that data, irrespective of whether those obligations are imposed on such providers for reasons of national security.</p> <p>The AG also recommended that the joined cases of Tele2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for Home Department v Tom Watson and Others (C-698/15) should be upheld, opining that a general and indiscriminate retention of all traffic and location data of all subscribers and registered users is disproportionate.</p>	15 January 2020	<p>Press release</p> <p>Link</p> <p>Opinion</p> <p>Link</p>
CJEU confirms right of access in marketing authorisation application cases	<p>The CJEU examined the right of access to documents in the context of marketing authorisation ("MA") applications in the judgments of PTC Therapeutics International Ltd v EMA (C-175/18 P) and MSD Animal Health Innovation and Intervet International v EMA (C-178/18 P).</p> <p>The CJEU concluded that the application of the general assumption of confidentiality by an institution, body or agency was merely an option, not an absolute obligation, provided that</p>	22 January 2020	<p>CJEU press release</p> <p>Link</p> <p>C-175/18 P judgment</p> <p>Link</p>



Development	Summary	Date	Links
	<p>the organisation conduct a specific, individual assessment of those reports to determine whether they are protected by any exceptions in Article 4 of Regulation 1049/2001.</p> <p>The CJEU then held that the specific risk of misuses of the data contained in a document to which access is sought must be established, meaning that a mere unsubstantiated claim of a general risk of misuses will not fall within the 'commercial interests' exception under Article 4(2) GDPR.</p> <p>Finally, the CJEU reasserted the principle of the widest possible right of access to documents held by EU institutions, bodies or agencies, and that the exception for the protection of commercial interests may only be applied for if the MA holder can establish that the disclosure of the documents in question would pose the risk of a concrete harm to the commercial interests of the persons whose data is concerned.</p>		<p>C-178/18 P judgment</p> <p>Link</p>
CJEU interprets data protection 'legitimate interests' as regards CCTV/video surveillance	<p>The CJEU in the Romanian case of TK v Asociația de Proprietari bloc M5A-ScaraA, has interpreted the lawful basis of 'legitimate interests' as regards CCTV/video surveillance. The video surveillance system in question was installed in the common parts of a residential building. The CJEU ruled that neither the Data Protection Directive nor the Charter of Fundamental Rights precluded national rules which authorised the installation of a video surveillance system such as for pursuing the legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects. The CJEU qualified this, requiring that the processing of personal data carried out by means of the video surveillance system at issue fulfills the conditions in the Data Protection Directive concerning 'legitimate interests'.</p>	28 January 2020	<p>Judgement</p> <p>Link</p>
European Commission NIS Cooperation Group provides toolkit on measures to mitigate security risks of 5G rollout	<p>The European Commission has endorsed a toolbox of measures agreed by Member States – through the NIS Cooperation Group – to mitigate security risks relating to the rollout of 5G.</p> <p>The toolbox recommends that Member States should implement measures to respond appropriately and proportionately to present and future risks, and restrict, prohibit and/or impose specific</p>	29 January 2020	<p>Press release</p> <p>Link</p>



Development	Summary	Date	Links
	<p>requirements for the supply, deployment and operation of 5G networks. In particular, Member States should:</p> <ul style="list-style-type: none"> – strengthen security requirements for mobile network operators (e.g. strict access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.); – assess the risk profile of suppliers; as a consequence, apply relevant restrictions for suppliers considered to be high risk for key assets defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions); – ensure each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile), ensure an adequate balance of suppliers at national level and avoid dependency on suppliers considered to be high risk. <p>The toolbox also recommends that the Commission should:</p> <ul style="list-style-type: none"> – contribute to maintaining a diverse and sustainable 5G supply chain; and – facilitate coordination between Member States regarding standardisation to achieve specific security objectives and developing EU-wide certification schemes. <p>The Commission has called for Member States to implement the measures by 30 April 2020 and to prepare a joint report on their implementation by 30 June 2020.</p>		
ENISA publishes report on implementation of European telecom code	<p>The European Union Agency for Cybersecurity (“ENISA”) published a report to support EU member states in their implementation of the European Electronic Communications Code. The report highlighted <i>inter alia</i> that the Code: provides an EU-wide definition of security requirements and incidents in the telecoms sector which includes breaches of confidentiality of communications and users’ authentication; allows authorities to require providers to mitigate significant threats; and covers over-the-top services like WhatsApp and Gmail.</p>	28 January 2020	<p>Press release Link Report Link</p>



Development	Summary	Date	Links
EDPB publishes documents adopted at 17th plenary	<p>The EDPB announced the outcomes of its 17th plenary meeting which took place on 28–29 January 2020. During the session, the EDPB adopted:</p> <ul style="list-style-type: none"> – its Opinions on the Accreditation Requirements for Codes of Conduct Monitoring Bodies (submitted to the Board by the Belgian, Spanish and French supervisory authorities (“SAs”) pursuant to Article 41 GDPR) – draft Guidelines 1/2020 on the processing of personal data in the context of connected vehicles and mobility related applications for consultation, ending 20 March 2020; – final version of the Guidelines 3/2019 on processing of personal data through video devices following public consultation; – Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 GDPR; – Opinion 5/2020 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 GDPR; – Opinion 6/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group); <p>The EDPB adopted a letter to MEP Sophie in’t Veld on the use of unfair algorithms, which provides an analysis of the challenges posed by the use of algorithms, an overview of the relevant GDPR provisions and existing guidelines addressing these issues, and describes the work already undertaken by SAs.</p> <p>The EDPB also adopted a letter to the Council of Europe Cybercrime Committee’s (T-CY) Octopus Conference stressing the need to integrate strong data protection safeguards into the future Additional Protocol to the Convention and to ensure its</p>	28 January 2020	<p>Press release Link</p> <p>Agenda Link</p> <p>List of adopted documents Link</p>



Development	Summary	Date	Links
	<p>consistency with Convention 108, as well as with the EU Treaties and Charter of Fundamental Rights.</p> <p>Finally, the EDPB adopted a document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal.</p>		
US Department of Commerce issue updated FAQs regarding Privacy Shield post-Brexit	<p>The International Trade Administration of the US Department of Commerce has issued an updated version of the FAQs relating to the EU-US Privacy Shield in the wake of Brexit. The FAQs particularly focus on the obligation on Privacy Shield organisations to update their public commitment of compliance with the Privacy Shield to specifically include the UK. The updated FAQs also outline that it is imperative for organisations to maintain a Privacy Shield certification and re-certify themselves each year.</p>	31 January 2020	<p>FAQs</p> <p>Link</p>
ENISA publishes cyber security standards reports	<p>ENISA has published:</p> <ul style="list-style-type: none"> – a report on standardisation in support of cybersecurity certification including a set of recommendations for Standards Developing Organisations and prospective authors of certification schemes; and – a report on standards supporting certification covering 5 areas (internet of things, cloud, threat intelligence in the financial sector, electronic health records and qualified trust services) in which frameworks, schemes or standards currently exist that could potentially be evolved to EU candidate cybersecurity certification schemes. <p>As a reminder, the Cybersecurity Act entered into force in the EU on 27 June 2019 and, among other things, establishes a cyber security certification framework which creates a mechanism and consistent set of rules for establishing various EU-wide cyber security certification schemes. While the UK Government plans to repeal the Cybersecurity Act post Brexit transition, it is expected to enter into negotiations with the EU, as part of its future relationship, to ensure that UK-issued cybersecurity certificates serve the same purpose in EU markets as EU-issued certificates</p>	4 February 2020	<p>Report on Standardisation in support of Cybersecurity Certification</p> <p>Link</p> <p>Report on Standards Supporting Certification</p> <p>Link</p>



Development	Summary	Date	Links
	and vice versa. For this reason, these reports may influence the UK's approach to cybersecurity certification.		
European Parliament warns Commission of deficiencies in UK privacy laws ahead of adequacy assessment	<p>In its proposed UK/EU negotiation mandate (paragraphs 32-34), the European Parliament recommended that the European Commission should carefully assess the UK's data protection legal framework and ensure the UK has resolved the following prior to considering UK data protection law adequate in line with EU law:</p> <ul style="list-style-type: none"> – immigration exemption in DPA 2018 (Schedule 2 Part 1 paragraph 4); – UK's legal framework on the retention of electronic telecommunications data; and – UK's legal framework on national security and processing by law enforcement authorities, particularly mass surveillance programmes which may not be adequate when considering <i>Schrems</i> case and ECHR case law. 	12 February 2020	<p>European Parliament adopted text</p> <p>Link</p>
Documents adopted at EDPB's 18th plenary	<p>The EDPB has published details of the documents and subject matter covered at its 18th plenary which was held on 18 and 19 February 2020.</p> <p>The key document adopted in the session was the draft guidelines to provide clarification regarding the application of Articles 46(2)(a) and 46(3)(b) GDPR regarding transfers of personal data from EEA public authorities to public bodies in third countries or to international organisations, where not covered by an adequacy decision. The consultation on the draft guidelines ends on 6 April 2020.</p> <p>In addition, the EDPB adopted a statement on the privacy consequences of mergers in the wake of the planned acquisition of Fitbit by Google.</p> <p>The session also focused on whether and when the EDPB and individual data protection supervisory authorities should conduct a review of the GDPR as required by Article 97 GDPR. The EDPB acknowledged that despite the general success of the implementation of the GDPR over the past 20 months, there are still several concerns, for example the harmonisation of national</p>	20 February 2020	<p>Press release</p> <p>Link</p>



Development	Summary	Date	Links
	GDPR procedures. However, in conclusion, the EDPB asserted that at this time it would be premature to carry out an evaluation.		
Policy of indefinite retention of convicts' biometric data found to be unlawful in <i>Gaughran v UK</i>	The European Court of Human Rights ("ECHR") recently ruled in <i>Gaughran v United Kingdom (App No 45245/15) [2020] ECHR 45245/15</i> that a Northern Irish police service's policy of maintaining a record of photographs, fingerprints and DNA samples was unlawful. The indiscriminate nature of the policy amounted to a disproportionate interference of a convicted person's fundamental right to respect his private and family life. The court held that "the applicant's biometric data and photographs were retained without reference to the seriousness of his offence and without regard to any continuing need to retain that data indefinitely" and the unlikelihood of any potential evaluation of the policy "failed to strike a fair balance" between competing private and public interests.	19 February 2020	Judgement Link
ESRB emphasises the risk of cyber incidents to financial stability	The European Systemic Risk Board ("ESRB") issued a report on 'Systemic cyber risk' which highlights how a single cyber incident can develop into a systemic cyber crisis. The report explains that a systemic cyber crisis could threaten stability across the financial sector and cause material damage to the economy. The ESRB also sets out the estimated global costs of cyber incidents which range from \$45 billion to \$654 billion.	19 February 2020	Press release Link
EU Commission publishes new strategies on data and AI White Paper	<p>The European Commission revealed its new strategy on data and artificial intelligence ("AI"), as part of the EU's effort to trigger and develop a digital transformation in Europe – to bring about a 'genuine single market for data and tackle the problems identified through policy measures and funding' and to 'enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world'.</p> <p>In respect of AI, the Commission published a White Paper in which it declares that 'for Europe to seize fully the opportunities that AI offers, it must develop and reinforce the necessary industrial and technological capacities'. The White Paper proposes several policy options which aim to enable the development of secure and reliable AI systems and applications</p>	19 February 2020	Press release Link White Paper on Artificial Intelligence: a European approach to excellence and trust Link



Development	Summary	Date	Links
	in Europe. The White Paper highlights the need for an AI regulatory framework to enforce compliance with EU rules – particularly around fundamental rights and consumer rights.		
Croatian Presidency releases revised draft ePrivacy Regulation	<p>The Croatian Presidency of the Council of the European Union (“Presidency”) released a revised draft of the Regulation concerning the Request for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (the “Draft Regulation”) introducing changes to Articles 6 (Permitted processing of electronic communications data), 7 (Storage and erasure of electronic communications data) and 8 (Protection of end-users’ terminal equipment information).</p> <p>Among the proposed changes are the possibility to process metadata for legitimate interests pursued by the electronic service or network provider except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user. In addition, a new ground for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users’ terminal equipment where necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user’s terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user.</p> <p>The Draft Regulation provides that the end-user’s interests shall be deemed to override the interests of the service provider where: the end-user is a child; the service provider processes, stores or collects the information in order to determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing; or the storage or collection of the information by the service provider contains special categories of personal data.</p> <p>The Working Party on Telecommunications and Information Society (WP TELE) is due to meet twice in March to discuss the proposal, as follows:</p>	21 February 2020	Draft Regulation Link



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – 5 March: Presidency will present the proposal to the group and delegations will have an opportunity to ask for additional explanations/clarifications and to express their first reactions – 12 March: Presidency will lead an article-by-article examination of the proposal and will invite delegations to present their position on the changes and suggest further amendments. <p>The Presidency also plans to issue a further document at the beginning of March, addressing other possible modifications to the proposal – on issues such as scope of the Regulation – with a view to discussing it at the 12 March meeting.</p> <p>By way of background, despite continued efforts made by the Finnish Presidency of the Council of the EU to progress the proposal last year, EU member states were unable to agree a common position on the proposed legislation. The Croatian Presidency is now looking to progress the proposal during its presidency rotation.</p>		
EDPS publishes blog post on facial recognition and AI	<p>The EDPS published a blog post setting out the EU’s approach to facial recognition and AI. Among other things, the blog post highlights the importance of agreeing how to apply key GDPR principles such as data minimisation, accountability and transparency to AI technology as well as understanding the contrast between the principle of data minimisation and the concept of <i>Big Data</i>, and the criteria that research activities must meet to fall under the scientific research derogations provided by the GDPR.</p> <p>Additionally, the blog post discusses the use of facial recognition software to identify an individual in a public place and classes it as significantly more intrusive than face authentication to unlock one’s smartphone.</p>	21 February 2020	Blog post Link
ENISA publishes cybersecurity procurement guidelines for hospitals	<p>ENISA has published its guidelines on cybersecurity in the context of procurement of services, products and infrastructure by hospitals.</p>	24 February 2020	Press release Link



Development	Summary	Date	Links
	<p>The guidelines:</p> <ul style="list-style-type: none"> – identify types of procurement and the corresponding assets relevant to hospitals' cybersecurity infrastructure, and outline the potential threats, risks and challenges related to procurement in hospital organisations; – emphasise that given the high sensitivity of medical data and the potential vulnerability of the healthcare sector, cybersecurity mechanisms should be implemented in every step to safeguard patient data privacy and the resilience of healthcare services; and – propose a set of good practices to meet the relevant cybersecurity objectives. 		<p>Guidelines</p> <p>Link</p>
WEF publishes white paper on facial recognition	<p>The World Economic Forum ("WEF") published its <i>Framework for Responsible Limits on Facial Recognition</i> white paper which provides a policy basis for the safe and ethical use of facial recognition technology.</p> <p>The white paper encourages organisations who are trialling facial recognition to carry out a number of precautionary steps including conducting impact assessments, designing systems to support privacy and establishing a process for informing end users on the use of facial recognition technology. Organisations are also recommended to obtain consent from individuals in respect of the use of facial recognition technology and retention of data derived from it.</p> <p>The white paper includes four main steps to ensure the responsible design and use of facial recognition technology for flow management use cases: <i>Define</i> what constitutes the responsible use of facial recognition through the drafting of a set of principles for action; <i>Design</i> a set of methodologies, tailored by use cases, to support product teams in the development of systems "responsible by design"; <i>Assess</i> to what extent the system designed is responsible through an assessment questionnaire that describes for each use case what rules should be respected to comply with the principles for action; and <i>Validate</i> compliance with the principle for action through the design of an audit framework by a trusted third party.</p>	February 2020	<p>WEF white paper</p> <p>Link</p>



Development	Summary	Date	Links
	The WEF concludes that the next steps of the project are to test the framework, assess its relevance and review this based on the results.		
European Data Protection Supervisor publishes 2019 annual report	<p>The EDPS, Mr Wojciech Wiewiórowski, has released the annual report for 2019. The report mainly summarises the achievements of the previous four years, as 2019 was the final year in a five year mandate.</p> <p>Throughout 2019, actions were taken to ensure that Regulation (EU) 2018/1725 was implemented which related to the protection of natural persons in terms of the processing of personal data by the Union institutions, bodies, offices and agencies on the free movement of such data. Investigations into the processing of personal data by EU institutions has also been carried out. The report also includes reference to security and EU borders, activities on the ground and international affairs. The EDPS mentions that the next task will be to ensure the new EU data protection rules deliver the promised results.</p>	18 March 2020	<p>Report</p> <p>Link</p>
C-PROC provides update on global state of cybercrime legislation	<p>The Cybercrime Programme Office of the Council of Europe (“C-PROC”) provided an update on the global state of cybercrime legislation. By February 2020, 55% of United Nations members had implemented local legislation to criminalise offences against and by means of computers which comply with the Budapest Convention on Cybercrime, that aims to define the conduct constituting criminality and establish evidence gathering powers which meet human rights and rule of law safeguards.</p> <p>In particular, good progress was noted in Africa. A greater number of states legislation have also adopted cybercrime investigative and evidence-gathering powers. Despite positive trends, C-PROC stated that further capacity building to ensure the application of legislation by criminal justice practitioners.</p>	20 March 2020	<p>Press release</p> <p>Link</p> <p>Update</p> <p>Link</p>
ENISA calls for experts in AI cybersecurity	<p>ENISA has launched a call for an Ad Hoc Expert Group on AI with the aim of bringing together a multi-disciplinary group of experts to advise ENISA on AI-specific cybersecurity topics. The Group will provide input on the following:</p> <ul style="list-style-type: none"> – AI cybersecurity; 	24 March 2020	<p>Press release</p> <p>Link</p> <p>Application page</p> <p>Link</p>



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – AI explainability and trustworthiness; – AI risk management; – Sectorial AI expertise; – Algorithmic security; – Data security in relation to AI; – AI cybersecurity; and – AI explainability and trustworthiness. <p>The deadline for applications is 18:00 CET on 15 April 2020.</p>		
Insurance Europe publishes its response to EDPB's guidelines on connected vehicles	<p>Insurance Europe has published its response to the EDPB draft <i>Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications</i> which is currently under public consultation. It called for several clarifications to be made, in particular that the guidelines should be revised to reflect a better understanding of insurance telematics and recognise the equal footing of all legal bases under GDPR that will allow insurers to access and process data from connected vehicles. Additionally, the guidelines should adopt greater flexibility in insurer's access to raw data which will allow them to provide innovative telematics products.</p>	25 March 2020	<p>Press release Link</p> <p>Response Link</p>
IAB Europe publishes its transparency guide for advertising supply chain	<p>The Interactive Advertising Bureau ("IAB") Europe released its updated Transparency Guide for the Digital Advertising Supply Chain ("Guide"). The aim of the Guide is to improve transparency in the digital advertising supply chain in specific areas of data, cost and inventory source. The Guide also provides questions for key stakeholders to bear in mind at different stages of the supply chain, particularly in relation to the provision of consent under the GDPR, cookies usage and consent management providers.</p> <p>In addition to the Guide, IAB Europe hosted a webinar which provides a deep dive into the Guide.</p>	26 March 2020	<p>Press release Link</p> <p>Guide Link</p> <p>Webinar slides Link</p> <p>Webinar recording Link</p>
ENISA publishes white paper on cybersecurity skills development	<p>ENISA has published a white paper on cybersecurity education and provided considerations and recommendations for policy</p>	26 March 2020	<p>Press release</p>



Development	Summary	Date	Links
	<p>actions at the national and European level to implement cybersecurity skills development. Further areas of research are also being considered to identify the nature and extent of the EU cybersecurity skills shortage.</p> <p>The white paper further addresses:</p> <ul style="list-style-type: none"> – The policy challenge of the cybersecurity skills shortage; – The causes of the shortage; – The processes and criteria established by 4 countries in order to certify cybersecurity degrees and the implications of establishing certification for cybersecurity degrees; – The creation of the ENISA's Cybersecurity Higher Education Database; and <p>Recommendations for increasing the number of graduates with the right cybersecurity knowledge and skills.</p>		Link
European Medicines Agency publishes Regulatory Science Strategy to 2025	<p>The European Medicines Agency published its Regulatory Science Strategy to 2025, which outlines its key areas of focus over the next five years.</p> <p>The strategy contains proposals relating to the handling of large volumes of data support the entry of precision medicines into public healthcare systems, the use digital tools in the implementation of new technologies and the establishment of an AI forum.</p>	31 March 2020	<p>Press release Link</p> <p>Strategy Link</p>



Austria

Contributors



Georg Roehsner
Partner

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



Manuel Boka
Senior Associate

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
Federal Administrative Court: Austrian Rules on Video Surveillance violate GDPR and are therefore declared void	<p>The Austrian Data Protection Act ("Datenschutzgesetz – DSG") contains detailed provisions on video surveillance, which in some parts are stricter than the GDPR.</p> <p>In two decisions, the Austrian Federal Administrative Court has ruled that the provisions under the DSG violate the GDPR as the GDPR does not allow Member States to institute stricter rules for video surveillance in a private context unless where this is explicitly stated in the GDPR. Therefore, the rules of the DSG on video surveillance have been declared void – at least in relation to video surveillance by individuals and by non-public entities.</p> <p>The Austrian Data Protection Authority ("DPA") has confirmed that following these judgements, it will deem the relevant provisions in the DSG to be void. Going forwards cases of video surveillance carried out in a private context (individuals and companies) will only be assessed under and in line with the GDPR.</p>	22 January 2020	<p>First Decision by the Federal Administrative Court (in German) Link</p> <p>Second Decision by the Federal Administrative Court (in German) Link</p>
Austrian DPA: Rules on dashcams under GDPR	<p>In the last edition of Updata, we informed you about a decision by the Austrian DPA, declaring most dashcam surveillance to be in violation of the GDPR.</p>	23 January 2020	<p>Guideline by the DPA (in German) Link</p>



Development	Summary	Date	Links
	<p>Following this, the Austrian DPA has issued a general guideline for the permissibility of dashcam surveillance under GDPR. Dashcam surveillance must (in short) fulfil at least the following criteria:</p> <ul style="list-style-type: none"> – The data processing is carried out for the exclusive purpose of documenting the course of an accident – The recording of the surrounding street and public area is limited to what is necessary. Large-scale surveillance of the vehicle's surroundings is prohibited. Camera resolution must be limited so that only a small area around the vehicle is clearly visible and persons or vehicles further away should not be identifiable; – Accident data may not be stored indefinitely, but only until the purpose has been achieved (i.e. retention of data in connection with an ongoing police investigation); and – The storage of image data may only be triggered (i.e. stopping of the overwriting process) automatically by predefined impulses (i.e. impact sensors, abrupt steering/driving/braking/acceleration manoeuvres), without the possibility of manual storage by the driver. 		
Austrian DPA: Online dating platforms must use "double opt-in" authentication	<p>In a recent decision, the Austrian DPA decided that the GDPR requires online dating platforms to use "double opt-in" procedures for registration on their website.</p> <p>"Double opt-in" means that after registering on the website, the user will receive an email (or a text message) with a further confirmation link. Only after clicking on this confirmation link will the registration be complete.</p> <p>In the underlying case, the platform had sent emails with containing explicit sexual content to the applicant. The applicant had never signed up to the platform. The platform claimed that an account had been opened using the applicant's email address, therefore emails had been sent to this email address. The platform had not used a double opt-in procedure to verify the identity of the registering person.</p> <p>The Austrian DPA ruled that under Art 32 GDPR, the platform provider is obliged to ensure that personal data cannot be used unlawfully on its platform. Therefore, platform providers</p>	30 January 2020	<p>Decision by the DPA (in German)</p> <p>Link</p>



Development	Summary	Date	Links
	areobliged to verify the identity of its users by a double opt-in procedure.		
Austrian DPA: Quarterly Report	The Austrian DPA has published its Quarterly Report focussed on the permissibility of video surveillance and the new Austrian Act on Passenger Name Records (PNR) based on EU-Directive 2016/681.	24 January 2020	Quarterly Report (in German) Link





China

Contributors



Jack Cai
Partner

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



Sam Chen
Senior Associate

T: +86 21 61 37 1004
samchen@
eversheds-sutherland.com



Jerry Wang
Associate

T: +86 21 61 37 1003
jerrywang@
eversheds-sutherland.com

Development	Summary	Date	Links
Provisions on Ecological Governance of Network Information Content (the "Provisions") (《网络信息内容生态治理规定》)	<p>On 15 December 2019, the Cyberspace Administration of China issued the Provisions which came into effect on 1 March 2020. The purpose of the Provisions is to protect the legitimate rights and interests of citizens, legal persons and other organizations, and safeguard national security and public interests.</p> <p>The Provisions have divided all network information into three main categories, with different regulations being applicable to individual categories. A network information content producer shall:</p> <ul style="list-style-type: none"> – be encouraged to produce, copy and publish information containing positive messages; – not make, copy or publish any illegal information; and – take measures to prevent and resist the production, reproduction and publication of undesirable information. <p>The Provisions also highlight duties and responsibilities of all relevant entities subject to it, namely: network information content producers, network information content service platforms, network information content service users, network</p>	<p>Publication Date: 19 December 2019</p> <p>Effective Date: 1 March 2020</p>	<p>Provisions on Ecological Governance of Network Information Content (in Chinese)</p> <p>Link</p>



Development	Summary	Date	Links
	industry organizations, and departments of cyberspace administration at different levels.		
GB/T 35273-2020 Information security technology – Personal information security specification (the “New Specification”) (GB/T 35273-2020 《信息安全技术 个人信息安全规范》)	<p>On 6 March 2020, the New Specification was jointly published by the State Administration of Market Regulation and the Standardization Administration of the People’s Republic of China, (taking effect 1 October 2020). The New Specification is an upgraded version of the specification currently in force, which has been in effect since 2017 (the “Current Specification”).</p> <p>The New Specification has brought about major changes, some of which are summarised below:</p> <ul style="list-style-type: none"> – Enhanced protections of personal biometric information; – Enhanced data subject’s ability to manage their personal information; – Improved compliance restrictions and regulations in relation to information integration and its use; and – Improved compliance restrictions and regulations in relation to commercialization of personal information. 	<p>Publication Date: 6 March 2020</p> <p>Effective Date: 1 October 2020</p>	<p>GB/T 35273-2020 Information security technology – Personal information security Specification (in Chinese)</p> <p>Link</p>



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 Lehuby
Associate

T: +33 1 55 73 42 09
camillelehuby@
eversheds-sutherland.com



Camille Larreur
Associate

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

Development	Summary	Date	Links
The CNIL releases new recommendations on consent for cookies	<p>On 14 January 2020, the CNIL issued draft recommendations providing practical guidance on the process for validly obtaining consent when implementing cookies.</p> <p>The recommendations complement the revised guidelines, setting out the applicable framework for cookies and tracking technologies, published by the CNIL on 4 July 2019 (see Updata edition 5).</p> <p>In this new guidance, the CNIL set out practical recommendations and best practices. Some highlights are summarised below:</p> <ul style="list-style-type: none"> – Informed consent: The CNIL recommends distinguishing between two levels of information to be provided to the users. Pursuant to this layered approach: (1) A first level of information, which must be provided to users before they give their consent which is to appear on the consent management interface itself. This first layer of information must include an exhaustive list of cookie purposes (with clear and concise descriptions), as well as a complete list of entities using cookies on the website or application (it is also permitted to use a hyperlink directing to the list, for example 	14 January 2020	<p>CNIL statement (in French) Link</p> <p>CNIL FAQ Link</p>



Development	Summary	Date	Links
	<p>if it is too long) and (2) A second level of information (which should be easily noticeable and accessible) where users receive more extensive descriptions of the purposes of the cookies. The list of controllers and a hyperlink to their respective privacy notices should also be provided, if not included in the first layer. Finally, the second layer must include information on the scope of the consent given (i.e. whether the consent given also covers other websites or apps).</p> <ul style="list-style-type: none"> – Free consent: The CNIL reiterates that a simple and clear mechanism should be made available to the users (via push buttons or unchecked boxes) to accept or refuse the implementation of cookies. Consent and refusal options should be displayed in the same manner on the consent management interface. <p>In addition, the refusal of the implementation of cookies should be recorded, in order to avoid repeatedly asking for consent during subsequent visits, which would lead to a certain form of pressure that may influence the users' decision.</p> <p>The CNIL also clarifies that, when users do not make a decision (e.g. close the consent management interface without having consented or refused cookies), editors are not allowed to implement any non-essential cookies on their devices.</p> <ul style="list-style-type: none"> – Specific consent: The CNIL allows editors to obtain a "bundled" consent for several purposes, provided that users are informed of all those purposes and are offered a bundled refusal option. Users should still be able to give granular consent for specific purposes (e.g. in the second layer of information). <p>The draft recommendations are subject to public consultation until 25 February 2020, a final version of the recommendation will be presented to the members of the CNIL meeting in plenary session for final adoption and the CNIL has announced that it will start enforcing its new cookies guidelines around the third quarter of 2020.</p>		



Development	Summary	Date	Links
The CNIL publishes a GDPR guide for web developers	<p>This guide provides best practices and guidance in implementing the GDPR, particularly regarding the main principles of the GDPR and the development of applications that respect its users' privacy.</p> <p>The guide includes 16 pages that cover the developers' needs at each stage of their project, including themes such as "securing the development environment", "manage the source code", "secure websites, applications and servers", "minimise the data collected", "taking the legal bases into account in the technical implementation", or "measuring website and application traffic".</p>	28 January 2020	<p>CNIL statement (in French)</p> <p>Link</p>
Good data protection practices for delinquency prevention at the communal level	<p>Prior to the entry into force of the GDPR, the processing of personal data implemented in the context of crime prevention by town halls was subject to a simplified authorisation process (Standard AU-38). This process no longer applies following entry into force of the GDPR since this type of data processing is no longer subject to authorisation, but remains a useful framework for townhalls to access the legality of data processing.</p> <p>In addition, the CNIL published recommendations regarding the 5 most frequently encountered shortcomings in the context of the data processing carried out by town halls for the prevention of petty crimes:</p> <ol style="list-style-type: none"> 1. Systematic collection of sensitive data or data relating to offences and security measures. Such data should be collected only when they are indispensable for the monitoring of the data subject. For example, for the examination of the situation of a minor sentenced to community service, the reason for the conviction is not necessary for the implementation of the monitoring. 2. Inserting open data fields in the monitoring sheets without strictly controlling their content. The use of open data fields encourages excessive data collection, purely subjective or inappropriate comments. 3. Keeping individual or collective monitoring files indefinitely. Data should be kept only for the time strictly necessary for monitoring the data subject. 	1 January 2020	<p>CNIL recommendations (in French)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>4. Lack of information to data subjects about the processing of their data. Individuals must be informed of the processing of their data for the purposes of crime prevention.</p> <p>5. A security flaw in data access. Given the sensitive nature of the data processed and the public concerned, access to the data must be strictly limited to legitimate persons who need to know the data because of their duties.</p>		
The CNIL releases new content dedicated to codes of conduct and Binding Corporate Rules ("BCRs").	<p>In order to assist organisations to implement codes of conduct or BCRs, the CNIL published guidance in understanding these compliance tools, and implemented a teleservice to submit BCRs to the CNIL. A teleservice for the approval of codes of conduct will also be implemented soon.</p> <p>This will provide recommendations on the content to include in the code of conduct, on the body in charge of monitoring compliance to the code of conduct, and on the approval process.</p> <p>The page dedicated to BCRs explains the purpose of implementing BCRs, and provides guidance on how to prepare the BCR submission to the supervisory authority.</p>	7 February 2020	<p>CNIL statement (in French) Link</p> <p>Codes of conduct page (in French) Link</p> <p>BCRs page (in French) Link</p>
Recommendations of the French government regarding spam emails	<p>The French government issued guidance on responding to spam emails. It cautioned that most spam emails are often direct marketing messages but some may be malicious.</p> <p>These recommendations include using the right to object, reporting the message to Signal Spam (a website managed by the CNIL) to help the CNIL to carry out controls, and filing a complaint with the CNIL or the police.</p> <p>The government also reminds that spam emails may constitute the following offences subject to fines and imprisonment:</p> <ul style="list-style-type: none"> – direct marketing without consent – unfair commercial practice – fraud – deception in commercial matters 	26 February 2020	<p>Government recommendations (in French) Link</p>



Development	Summary	Date	Links
	It must be noted that the French Criminal Code provides that fines can be multiplied by five for legal entities.		
Facial recognition experiment in high schools found illegal	<p>The administrative court of Marseille assessed the lawfulness of the installation of facial recognition systems (two portals at the entrance of the premises) in two high schools of Marseille and Nice.</p> <p>The regional council was responsible for the installation and its decision was challenged by associations made up of parents and of teachers.</p> <p>The administrative court decided that the regional council's decision was unlawful considering:</p> <ul style="list-style-type: none"> – the installation was intended to improve safety in schools but did not fall within the remit of the regional council of "reception, accommodation or maintenance of secondary schools", but within the high school director's remit of "supervising and monitoring pupils". The regional council was therefore not competent to decide installation; – the processing relied on consent without sufficient safeguards to ensure that the students and their legal representatives were giving free and informed consent; – that the regional council was not demonstrating that the purpose of the processing which was to ease and secure security controls at the entrances of the school constituted a reason of public interest, and could not be achieved in a sufficiently effective manner by badge controls, accompanied, if necessary, by the use of video surveillance. 	27 February 2020	<p>Court decision (in French)</p> <p>Link</p>
The CNIL launches a public consultation on its "Data Protection Training" certification project	<p>The CNIL no longer delivers its label "Training" since the entry into force of the GDPR. However, the GDPR has reinforced the need for training on protection of personal data.</p> <p>Numerous training courses have been created, either with a diploma or in a short format.</p> <p>In this context, the draft certification rules designed by the CNIL take into account the new legal framework for professional</p>	5 March 2020	<p>CNIL statement (in French)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>training while integrating the specificities relating to data protection.</p> <p>The CNIL will create a specific logo to facilitate the visual identification of service providers who have obtained this voluntary certification, and is currently working on the accreditation process for bodies that will be entitled to deliver the certification to training providers.</p> <p>The public consultation ended on 27 March 2020.</p>		
The CNIL announces its control strategy for 2020	<p>In 2020, the CNIL will focus its activities on three areas: (i) health data, (ii) geolocation for local services, and (iii) cookies and other tracers.</p> <p>Every year, the CNIL carries out thousands of investigations, into complaints, checks as part of the procedure for indirect right of access to certain administrative files, reports of personal data breaches or formal control procedures.</p> <p>These formal procedures, around 300 per year, make it possible to investigate complaints in greater depth, to react to topical issues, to ensure compliance with previous corrective measures or to investigate certain topics deemed to be priorities. In 2020, more than 50 of these formal procedures will be carried out in the framework of the three themes selected as priorities for the year.</p> <p>In addition, the entry into force of the GDPR has reinforced certain requirements, particularly on how to collect a free, informed, explicit and unambiguous consent. One of the consequences is that the mere continuation of browsing on a site can no longer reflect a valid consent of the user to the use of cookies.</p> <p>The CNIL was thus led to adopt guidelines in July 2019 to clarify the new legal framework. In spring 2020, it will issue a recommendation (a public consultation was launched on the draft recommendation in January 2020) to guide operators in the application of the new requirements. It will give organisations six months from the publication of this recommendation to comply with the new obligations resulting from the GDPR. Controls on these new obligations will start in autumn 2020 and continue in 2021.</p>	12 March 2020	<p>CNIL statement (in French)</p> <p>Link</p>



Development	Summary	Date	Links
BYOD: the CNIL good practices	<p>The CNIL has issued recommendations for employers who are willing to implement a Bring Your Own Device ("BYOD") policy.</p> <ol style="list-style-type: none"> 1. Security measures. Employers are responsible for the security of their company's personal data, including when stored on devices over which they have no physical or legal control, but that they have authorised to access the company's IT resources. In order to reduce risks to IT systems, the CNIL recommends: <ul style="list-style-type: none"> – Identifying the risks, taking into account the context prioritise them according to severity and likelihood; – Determining the measures to be implemented and formalise them in a security policy. <p>The following measures may be considered:</p> <ul style="list-style-type: none"> – compartmentalise the parts of the personal device that are intended to be used in a professional context; – controlling remote access by means of a robust user authentication device; – implement encryption measures for information flows; – provide for a procedure in the event of failure/loss of the personal device; – require compliance with basic security measures such as locking the device with a password in accordance with good practice; – make users aware of the risks, formalise the responsibilities of each person and specify the precautions to be taken in a binding charter. 2. Safeguards for privacy. The security of the company's IT system must be reconciled with respect for the privacy of employees who use personal equipment in the course of their work. <p>While the employer may provide for remote deletion of the part of the personal terminal specifically dedicated to remote access to the company's resources, he may not,</p> 	24 March 2020	<p>CNIL recommendations (in French)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>on the other hand, assume the right to remotely erase all the data present on the employee's terminal.</p> <p>3. Compliance. BYOD is not a particular type of processing per se but only a channel facilitating the processing of data. Therefore, using BYOD does not change the obligations to which employers are subject, such as registration in the record of data processing activities and data protection impact assessments.</p>		
Publication of a decree authorising the French Ministry of Justice to create an automated personal data processing method named "DataJust"	<p>This decree authorised the French Ministry of Justice to create an automated personal data processing method named "DataJust" for the purpose of developing an algorithm designed to enable:</p> <ul style="list-style-type: none"> – the retrospective and prospective evaluation of public policies on civil and administrative liability; – the development of an framework for the compensation of personal injuries; – the provision of information to the parties in order to help them to assess the amount of compensation to which victims are entitled in order to encourage an amicable settlement of disputes; and – the provision of information or documentation to judges called upon to rule on claims for compensation of personal injuries. <p>The decree provides that the personal data to be processed will be extracted from court decisions handed down on appeal between 1 January 2017 and 31 December 2019 by the administrative and the civil chambers of judicial courts in disputes relating solely to compensation for personal injury.</p>	29 March 2020	<p>Decree No. 2020-356 of 27 March 2020 creating an automated processing of personal data called "DataJust" (in French)</p> <p>Link</p>



Germany

Contributors



Alexander Niethammer
Partner

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



Lutz Schreiber
Partner

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



Nils Müller
Principal Associate

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



Constantin Herfurth
Associate

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



Sara Ghoroghy
Associate

T: +49 40 80 80 94 446
saraghoroghy@
eversheds-sutherland.com



Philip Kuehn
Associate

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

Development	Summary	Date	Links
Bavarian Data Protection Authority assumes that potential employers are not allowed to inform themselves about applicants on Facebook	In the opinion of the Bavarian Data Protection Authority a requirement within the meaning of Section 26 (1) of the German Federal Data Protection Act (" BDSG ") states that this would only be assumed to be necessary for those sources on the Internet that have a professional connection (e.g. XING or LinkedIn), because members of these networks post information about themselves in a professional context.	31 January 2020	9th activity report of the Bavarian State Office for Data Protection Supervision for the year 2019 Link
Bavarian Data Protection Authority publishes statement regarding adequacy of Privacy Shield	The Bavarian data protection authority has confirmed that the Privacy Shield Decision of 2016 provides an adequate level of data protection in the sense of Article 45 GDPR. The certification is valid for one year and can be renewed at the US Department of Commerce.	31 January 2020	9th activity report of the Bavarian State Office for Data Protection Supervision for the year 2019 Link



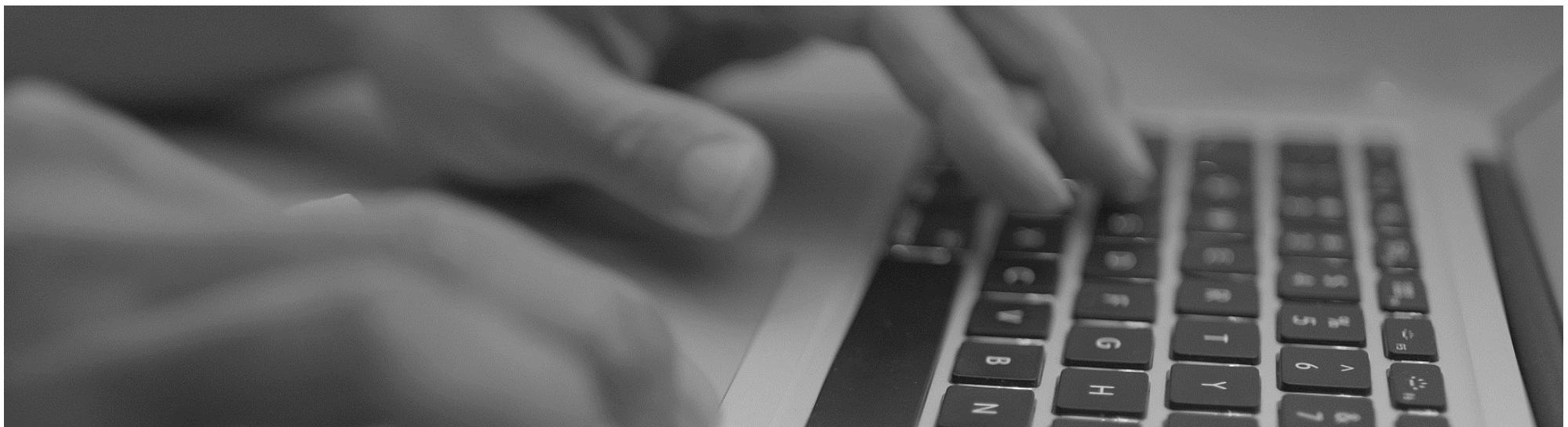
Development	Summary	Date	Links
Bavarian Data Protection Authority publishes statement regarding the use of “Google Analytics” or other tracking services without consent	In the opinion of the Bavarian Data Protection Authority, website operators who track users by using Google Analytics or other tracking services without obtaining the user’s prior consent commit a data protection violation that can be punished with a substantial fine. In addition to the question of the legality of the use, the website operator should also check whether he has informed users sufficiently about tracking services in its privacy policy.	31 January 2020	9th activity report of the Bavarian State Office for Data Protection Supervision for the year 2019 Link
Data Protection Authority of Hamburg publishes statement regarding joint responsibility for the use of Google Analytics	In its annual report, the Data Protection Authority of Hamburg tackled the issue of Google Analytics. In its opinion, an exclusion of the GDPR is not possible, even by shortening the IP addresses. Furthermore, Google and the Website Provider have to enter into a data processing agreement pursuant to Art. 28 GDPR and also into a joint controller agreement.	13 February 2020	28th activity report of the Hamburg Representative for data protection and freedom of information for the year 2019 Link
Bavarian Data Protection Authority publishes new guidelines on the usage of video surveillance by public agencies	The Bavarian Data Protection Authority published a comprehensive orientation guideline which summarizes and further develops his many years of consulting practice. Two additionally provided forms enable Bavarian public bodies to carry out structured checks and documentation of video surveillance. The guidelines help facilitate the application of legal requirements regarding video surveillance.	1 February 2020	Bavarian Data Protection Authority guidelines Link
The German Federal Office for Information Security (BSI) publishes a new catalogue of requirements regarding security criteria for smartphones	The security catalogue aims to improve the data security of users of digital services. The catalogue is addressed to smartphone producers, mobile phone providers and original equipment manufacturers. The catalogue describes criteria to protect mobile devices with special hardware features and to strengthen the software in its delivery state.	25 February 2020	BSI catalogue of requirements regarding security criteria for smartphones Link
OLG Stuttgart decides that a violation of the information obligations under Art. 13 GDPR constitutes a violation of competition pursuant to the German Unfair Competition Act	The Higher Regional Court in Stuttgart decided that the standards of the GDPR, in particular Art. 13 GDPR, have a reference to the sales market and therefore their violation constitutes a claim for injunctive relief under the German Unfair Competition Act (“ UWG ”). The court based its decision on the fact that it may also be important for a consumer, when initiating a transaction, for which purpose his data is to be processed and for how long it is to	27 February 2020	OLG Stuttgart decision Link



Development	Summary	Date	Links
	<p>be stored. This applies all the more if the consumer discloses his data in the case of a free or low-cost service in exchange. However, the question of whether GDPR infringements can be prosecuted under the UWG has not yet been finally clarified. The courts are currently still in disagreement and a final decision by the highest court, the Federal Supreme Court, is still to be made.</p>		
Data Protection Authority of Baden-Württemberg publishes statement regarding data processing by artificial intelligence	<p>Pursuant to the Data Protection Authority of Baden-Württemberg, the processing of personal data (such as vehicle registration numbers or persons on the pavement) by autonomous driving is permitted under Article 6(1) (f) of the GDPR, since the balancing of interests is in favor of the party processing the personal data. The Authority argued that only a small group of persons with access rights exists, the duration and territorial range of processing is not extensive, and the personal data is not disclosed to third parties. In addition, the rights of the persons concerned are safeguarded by ensuring that the recording vehicles are equipped with camera icons and the information about the responsible persons are marked. This allows the concerned data subjects to make use of their right to object to the data processing.</p>	20 January 2020	<p>Statement by the Data Protection Authority of Baden-Württemberg</p> <p>Link</p>
Hessian Data Protection Authority releases statement on the scope of the right of access and the access to patient files	<p>The Hessian Data Protection Authority releases a statement on the distinction of the right of access pursuant to Art. 15 GDPR and the right to access patient files pursuant to s 630 g the German Civil Code. The Authority clarifies that under Art. 15 GDPR, a data subject has the right to access their personal data. However, this access right does not extend into a right to be provided with copies of all relevant documents and files where such information might be contained. This is much rather covered by s 630 g BGB.</p> <p>Both rights are independent from each other as the legislator had different purposes in mind whilst drafting each provision. s 630 g BGB is not supposed to restrict Art. 15 GDPR as it is supposed to protect other interests patients might have distinct from the interests protected under Art. 15 GDPR.</p>	11 March 2020	<p>Statement by the Hessian Data Protection Authority</p> <p>Link</p>



Development	Summary	Date	Links
LG Heidelberg decides there is no right to information according to the GDPR if the effort is too high.	In the opinion of the LG Heidelberg (Regional Court in Heidelberg), there is no right to information according to Art. 15 GDPR if the effort involved is disproportionate (here: review and blackening of approx. 10,000 e-mails). The information interest of the requesting party and the economic interests of the recipient must be carefully weighed against each other. In the present case, adequate information would have cost the defendant EUR 4,000 and tied up his resources for several weeks. This is a case of disproportionality.	6 February 2020	
No right to erasure of personal data against the public prosecutor.	The Bavarian Supreme Court (BayOLG) has ruled that no right of erasure against a public prosecutor's office exists as long as the criminal offence on which the preliminary proceedings are based is not time-barred. The interest of the law enforcement authorities in storing the data takes precedence over the interest of the accused in avoiding stigmatisation. Deletion shall only be carried out when the preliminary proceedings has been completed, i.e. in the case of a discontinuation of proceedings according to paragraph 170 (2) of the German Code of Criminal Procedure with the commencement of the limitation period.	27 January 2020	Court decision 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



Duncan Watt
Consultant

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



Rhys McWhirter
Consultant

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



Wing Chan
Senior Associate

T: +852 2186 3223
wingchan@**eversheds-**
sutherland.com



Jamie Leung
Solicitor

T: +852 2186 4987
jamieleung@
eversheds-sutherland.com



Phillip Chow
Associate

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

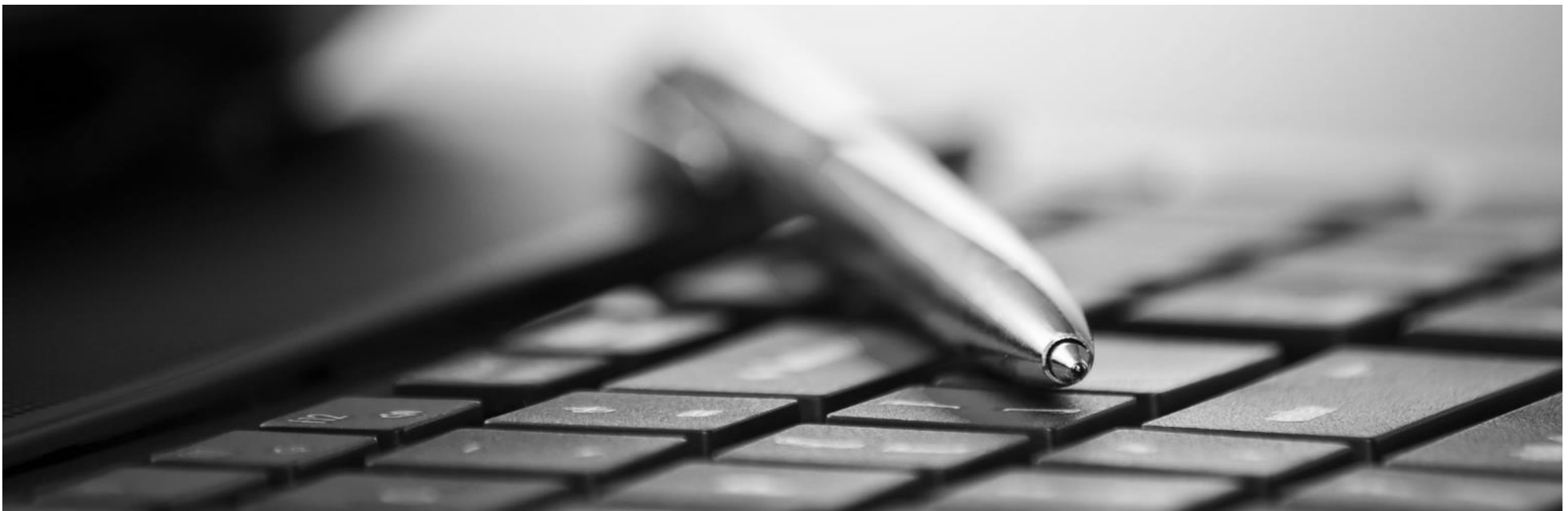


Maggie Lee
Trainee Solicitor

T: +852 2186 4986
maggielee@eversheds-
sutherland.com



Development	Summary	Date	Links
The Legislative Council Panel on Constitutional Affairs released a discussion paper to propose amendments to the Personal Data (Privacy) Ordinance	<p>The proposed amendments to the Personal Data (Privacy) Ordinance (Cap. 486) (“PDPO”) focus on six specific areas:</p> <ul style="list-style-type: none">– Establishing a mandatory data breach notification mechanism;– Strengthening the regulation on data retention periods;– Imposing regulations on data processors directly;– Increasing penalties of non-compliance with the PDPO;– Revising the definition of “personal data” to include “identifiable” natural persons (rather than an “identified” persons), in part due to the more prevalent use of tracking and data analytics technology; and– Regulating doxxing (i.e. deliberate disclosure of personal data of other data subjects).	13 January 2020	Discussion Paper Link





Hungary

Contributors



Ágnes Szent-Ivány
Partner

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



Kinga Mekler
Associate

T: +36 1 394 31 21
mekler@
eversheds-sutherland.hu



Katalin Varga
Partner

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

Development	Summary	Date	Links
Resolution of the NADP No. NAIH/2020/32/4	<p>The Authority issued guidance in a case regarding uploading a photo to Facebook without consent. The uploader, a council member took a photo of an official representing a public body tearing down an ad of a political adversary and uploaded the photo without his consent.</p> <p>The authority concluded that “the official’s name was considered to be in the public interest at the time the image was taken and published. However, the applicant’s facial image could not be considered as that the appearance of a chairman (or member) of the board is not related to the discharge of public duties.”</p>	4 March 2020	<p>View the NADP resolution here (in Hungarian only). Link</p>



Ireland

Contributors



Marie McGinley
Partner

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



Fiona Lipsett
Solicitor

T: +35 31 64 41 47 0
fionalipsett@
eversheds-sutherland.ie



Neasa Ní Ghráda
Senior Associate

T: +35 31 66 44 25 8
neasanighrada@
eversheds-sutherland.ie

Kirsty Farrell
Trainee

T: +35 3 16 64 49 41
kirstyfarrell@
eversheds-sutherland.ie

Development	Summary	Date	Links
The Irish Data Protection Commission (the DPC) publishes blog on data protection on the Campaign Trail in the lead up to the Irish General Election	The DPC acknowledged the importance of politicians being able to stay connected to voters and members of their constituencies whilst also recognising the obligations and responsibilities imposed on those collecting personal data for electoral purposes as controllers. The article discussed the rights of individuals when their personal data is used for campaigning or electoral purposes and the obligations on those collecting the personal data for the same purposes. The article also included further information guides for both individuals and campaigners.	21 January 2020	DPC guidance Link
DPC provides guidance on 'opinions' and their data protection implications	This DPC blog recognised the balance between the right to freedom of expression and the right to data protection in respect of opinions that are recorded or processed through 'automated means'. The DPC noted that whether data protection law applies to an opinion, and if or how individuals' rights might be exercised regarding said opinion, will depend on the content and nature of the opinion.	24 January 2020	DPC guidance Link
DPC releases episode 10 in the 'Know Your Data' podcast series and focuses on data protection and elections	This episode centred on data protection in respect of elections. Again, the DPC acknowledged the importance of campaigners being able to contact voters in the run up to the Irish General Election, which took place on 8 February 2020. The podcast then	30 January 2020	DPC guidance Link



Development	Summary	Date	Links
	discussed the data protection rights that an individual is entitled to when their personal data is used for electoral purposes.		
DPC launches Statutory Inquiry into Google's processing of location data and transparency surrounding such processing	Following complaints from various consumer organisations across the EU, the DPC, as lead Supervisory Authority for Google, launched a Statutory Inquiry into the processing of location data by Google. The complaints surrounded the legality of Google's processing of location data and the transparency of such processing. Pursuant to section 110 of the Data Protection Act 2018, the DPC launched an own-volition Statutory Inquiry in accordance with the co-operation mechanism outlined under Article 60 of the GDPR.	4 February 2020	DPC guidance Link
DPC launches Statutory Inquiry into MTCH Technology Services Limited (Tinder)	The DPC stated that it had been actively monitoring complaints received from individuals in order to investigate and ascertain whether there have been thematic and systemic data protection issues. The DPC commenced an own-volition Statutory Inquiry pursuant to section 110 of the Data Protection Act 2018 and in accordance with the co-operation mechanism outlined under Article 60 of the GDPR. The inquiry will determine if Tinder has a legal basis for ongoing processing of personal data and whether Tinder complies with its obligations and responsibilities to its data subjects.	4 February 2020	DPC guidance Link
DPC provides guidance on operationalising accountability through Codes of Conduct and Certification	The DPC discussed the principles of accountability as provided by Article 5.2 of the GDPR and cast attention to the various mechanisms under the GDPR that organisations can adopt to demonstrate accountability. The DPC specifically mentioned (1) Codes of Conduct (Articles 40 and 41), and (2) Certification (Articles 42 and 43), which "will allow all stakeholders to play their part in the application, monitoring, supervision and enforcement of data protection standards". The DPC also commented on the public consultation on the processing of children's personal data and noted that it will soon be publishing its guidance. The DPC confirmed that the guidance will include a 'firm foundation' for the formation of Codes of Conduct for processing the personal data of children.	7 February 2020	DPC guidance Link



Development	Summary	Date	Links
DPC publishes responses to frequently asked questions on data protection and Brexit	The DPC sought to answer some of the questions and queries arising in the context of Brexit, particularly a 'no deal' scenario. This guidance sought to provide information to controllers on how Brexit may impact them and the steps they should take. This included information on the different mechanisms a controller can adopt when transferring data outside the EEA.	9 February 2020	DPC guidance Link
DPC publishes statement on Facebook dating feature	On 3 February 2020, Facebook Ireland Limited (Facebook) engaged with the DPC in respect of their intention to introduce a dating feature in the EU. The DPC raised concerns due to the fact that it was not provided with any information in respect of Data Protection Impact Assessments or the decision making processes undertaken by Facebook. Authorised Officers of the DPC attended the registered offices of Facebook on 10 February 2020 and gathered documentation. Facebook subsequently informed the DPC that they were postponing the roll-out of the dating feature.	12 February 2020	DPC guidance Link
DPC publishes 2019 Annual Report	The DPC published the annual report on the workings of the DPC during the first full calendar year of the GDPR. This report included an analysis of the current trends in complaints, breaches and legal issues faced by the DPC, investigations and inquiries launched by the DPC and current litigation and case studies. See our Spotlight on the highlights of the DPC Annual Report 2019 .	20 February 2020	DPC guidance Link Eversheds Sutherland article Link
DPC publishes statement on Facebook Election Day Reminder	Facebook Ireland Limited (Facebook) had intended to utilise a Facebook Election Day Reminder in the run up to the Irish General Election on 8 February 2020. The DPC informed Facebook that this feature raised a number of concerns around transparency to users including how their personal data is collected and used when interacting with this feature. The DPC sought to impose a number of remedial actions that Facebook would need to take in order to use this function. Facebook believed that it was not possible to implement these remedial actions in advance of the General Election and therefore refrained from using the feature. The matter is still ongoing.	27 February 2020	DPC guidance Link



Development	Summary	Date	Links
DPC provides guidance for organisers of conferences, workshops and events in respect of attendee lists and name tags	The DPC posted a blog regarding common GDPR misconceptions regarding name tags/badges and attendance lists. The DPC noted consent is not always needed nor the appropriate grounds for such processing purposes. The blog emphasised that the organiser should consider the reasonable expectation of the attendees.	28 February 2020	DPC guidance Link





Italy

Contributors



Massimo Maioletti

Partner

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

Edoardo Coia

Trainee

T: +39 06 89 32 70 34
edoardocoia@
eversheds-sutherland.it

Development	Summary	Date	Links
Publication of the final report of Italian Supervisory Authorities' joint investigation on Big Data	The Italian Data Protection Authority (" IDPA "), along with the Italian Competition Authority and the Italian Communications Authority, conducted a detailed investigation on Big Data. The final report highlighted each authority's point of view on the topic.	10 February 2020	Press release announcing the publication of the final report of the joint investigation on Big Data, containing a link to the report (in Italian only) Link
IDPA's Newsletter n. 462 of 18 February 2020	<p>The IDPA published its Newsletter, which highlighted the following issues:</p> <ol style="list-style-type: none"> 1. IDPA published its investigation plan for the first half of 2020. In particular, IDPA announced that its controls and audits will, address: <ul style="list-style-type: none"> – processing activities of personal data relating to health performed by multinational companies of the pharma and health sector; – processing activities of personal data performed in the context of online banking services; – processing activities of personal data performed through whistleblowing applications; – processing activities of personal data performed by companies for marketing activities; – processing activities of personal data performed by companies with reference to profiling activities of fidelity cards' subscribers; 	18 February 2020	<p>IDPA's Newsletter n. 462 of 18 February 2020, including other measures by IDPA (newsletter and included documents only available in Italian language) Link</p> <p>IDPA's investigation plan for the first half of 2020, included in the Newsletter n. 462 of 18 February 2020 Link</p> <p>IDPA's measure n. 17 of 23 January 2020, included in the Newsletter</p>



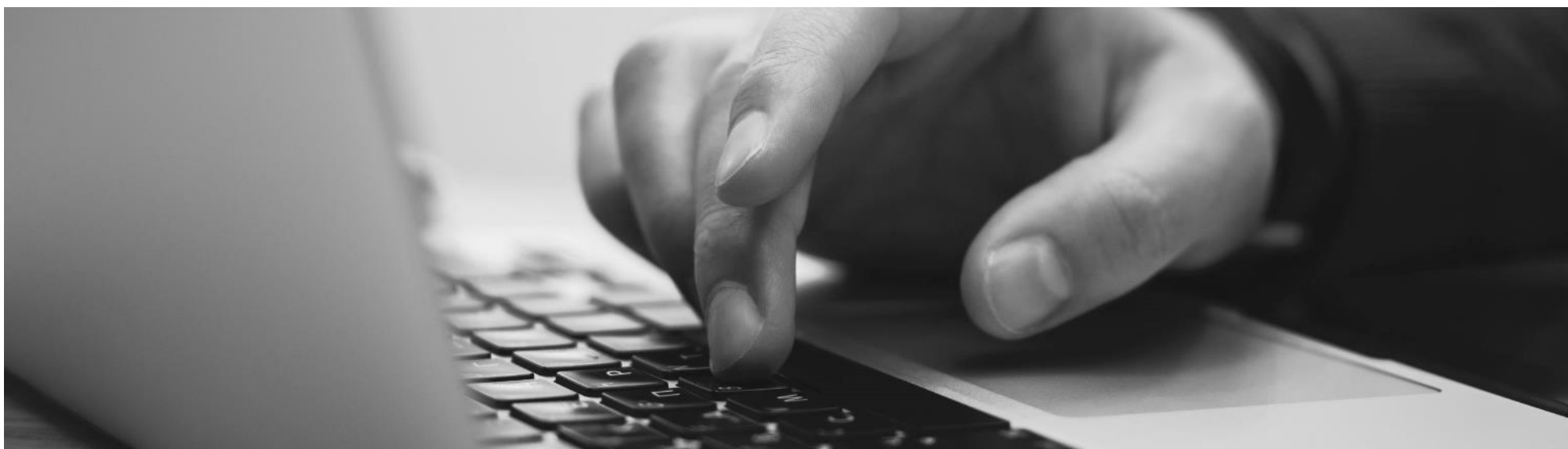
Development	Summary	Date	Links
	<ul style="list-style-type: none"> – processing activities of personal data performed by Food Delivery companies; – data breach. <p>In addition, the IDPA plans to verify the compliance of private and public entities, belonging to homogeneous clusters, with:</p> <ul style="list-style-type: none"> – the conditions of lawfulness of the processing and of the collection of consent (where the processing is grounded on that legal basis); – the obligation to provide an information notice; and – the principle of storage limitation. <p>In any case, the IDPA may perform further investigation activities, both ex officio and with reference to reports and complaints lodged.</p> <p>2. The IDPA issued a fine against an Italian university after an investigation into a data breach notification made by the university. During a software update a technical issue occurred and personal data of persons who confidentially reported unlawful behaviours using the university's whistleblowing platform had accidentally been indexed on browsers and became available publicly online.</p> <p>The university reported to have solved the issue, but the IDPA found that the breach occurred due to the absence of appropriate technical and organisational measures being in place to control access and restrict access to authorized personnel only. The IDPA remarked that the obligation to implement appropriate technical and organisational security measures under Art. 32 GDPR includes the need to set a procedure to regularly test and assess the appropriateness of the measures adopted.</p> <p>In this case, the IDPA noted that the university maintained the whistleblowing application settings as configured by the application provider (this configuration provided neither for the encryption of personal data nor for the adoption of a transmission protocol able to ensure security in the communications). The IDPA found this breach particularly serious, due to the special protection reserved under the law</p>		<p>n. 462 of 18 February 2020</p> <p>Link</p> <p>IDPA's measure n. 18 of 23 January 2020, included in the Newsletter n. 462 of 18 February 2020</p> <p>Link</p>



Development	Summary	Date	Links
	<p>to whistleblowers, but took into account the university's collaborative behaviour, fining it for an amount of EUR 30.000.</p> <p>3. The IDPA fined a hospital for not having prevented unauthorised access by employees of health data belonging to colleagues. The employees accessed the data using the credentials of other colleagues, having no particular working reason for the access.. The hospital identified this level of access as data breaches and notified the IDPA, who consequently started an investigation. IDPA noted how technical and organizational measures adopted by the hospital were not appropriate to protect patients' data from unauthorized access. IDPA also noted that these breaches could have been avoided by merely complying with the guidelines on health documentation issued by the IDPA in 2015. These guidelines provided restrictions of access to patients' health documentation, limiting accesses to the sanitary personnel involved in the care of the patient to whom the documentation refers. IDPA noted how this restriction provision can currently be interpreted in light of the privacy-by-design and privacy-by-default principle. IDPA fined the hospital for an amount of EUR 30.000</p>		
IDPA's information page on smart assistants	<p>The IDPA published on its website an information page on the data protection implications relating to the usage of smart assistants. The IDPA provided data subjects with some indication to spread awareness on the usage of such devices, with a particular focus on the information that smart assistants can collect and on the chance to regulate and/or disable some of their functions in certain scenarios.</p>	4 March 2020	<p>IDPA's information page (only available in Italian language)</p> <p>Link</p>
IDPA's Newsletter n. 463 of 6 March 2020	<p>The IDPA published its Newsletter, which highlighted the following issues:</p> <ul style="list-style-type: none"> – IDPA issued a measure against an electronic signature service provider following investigations conducted in the second half of 2019. IDPA issued an emergency measure, published in March this year, to enable the provider to implement remedies in order to protect a large number of data subjects. IDPA found the following security risk areas: 	6 March 2020	<p>IDPA's Newsletter n. 463 of 6 March 2020 (newsletter and included documents only available in Italian language)</p> <p>Link</p>



Development	Summary	Date	Links
	<ul style="list-style-type: none">– that the provider hadn't imposed on its users to change the initial password to access to the service;– technical passwords to manage IT services were left available in actions logs, increasing risks; and– logs of messages exchanged by users could be consulted and exported through the internet, by using a profile used by multiple persons. <p>The IDPA collaborated with the Italian general contracting entity for the public sector to amend a number of public tenders relating to the purchase of medical devices in order to make them more privacy-complaint. The amendments considered measures to protect personal data processed and standard clauses, as the designation of the winning tenderer as data processor. In addition, requirements in relation to privacy-by-design and privacy-by-default principles were put in to current public tenders, both regarding the devices to be purchased and the information required to participate.</p>		IDPA's measure n. 228 of 18 December 2019, included in Newsletter n. 463 of 6 March 2020 Link





Lithuania

Contributors



Rintis Puisys
Partner

T: +370 5 239 2391
rimtis.puisys@
eversheds.lt



Akvilė Jurkaitytė
Associate

T: +370 5 239 2391
akvile.jurkaityte@
eversheds.lt

Development	Summary	Date	Links
Summary of court decisions in the field of personal data protection in 2019	<p>The State Data Protection Inspectorate ("SDPI") summarised the court decisions that dealt with the complaints of persons investigated by the SDPI.</p> <p><u>Video surveillance:</u></p> <ul style="list-style-type: none"> – The Vilnius Regional Administrative Court dismissed the applicant's complaint challenging SDPI's order to cease video surveillance outside its private territory. – The court ruled that the applicant did not ensure that the video surveillance field did not capture the territory of third parties, thereby violating the applicable requirements. <p><u>Collection of data without identifying the reporting subject:</u></p> <ul style="list-style-type: none"> – The Supreme Administrative Court of Lithuania dismissed the complaint of the applicant UAB Foodout.lt, challenging the order of SDPI to ensure the identification of the person ordering the food (by activating a link sent by e-mail or otherwise). – The dispute arose due to the fact that when entering the details of the person ordering the food (name, surname, address, etc.) on the website of Foodout.lt and later entering this data in the service order and invoice, it was not checked whether the data was entered by the owner of the data or not. 	8 January 2020	<p>SDPI summary (in Lithuanian)</p> <p>Link</p>



Development	Summary	Date	Links
	<p>Unlawful disclosure of data, failure to inform a person:</p> <ul style="list-style-type: none"> – The Supreme Administrative Court of Lithuania declared that SDPI was right to rule on a breach of data subjects' rights when a former employer (UAB) approached the employment agency requesting the contact details of a former employee needed for the trial and, in this case: <ul style="list-style-type: none"> – unfairly disclosing to a recruitment agency that the employee has been made redundant due to a serious breach of work discipline; – not informing the former employee of such processing of former employee data. 		
The State Data Protection Inspectorate has announced a list of preventive inspections for 2020	<p>The SDPI has announced which preventive inspections will be carried out in 2020. A total of 50 organisations are planned to be checked, focusing on 4 key areas:</p> <ul style="list-style-type: none"> – The scope of personal data processing in the financial sector, with regard to payment initiation services; – The extent of personal data processed by educational institutions to justify the reasons for non-attendance; – Ministries and their subordinate institutions with regard to the scope of personal data processed in information systems; – Online shops for the adequacy of the implemented personal data security measures when processing personal data for the purpose of providing goods and services. – Upon completion of preventive inspections, SDPI will publish a summary of recommendations. According to the SDPI, published recommendations will be relevant not only to the organisations inspected, but also to other companies within the sector which will be able to review the results of the inspections and improve their activities respectively. 	29 January 2020	<p>Full list (in Lithuanian)</p> <p>Link</p>



Malaysia

Contributors



Suaran Singh Sidhu
Partner

T: +603 9212 9287
suaransidhu@
law-partnership.com

Development	Summary	Date	Links
Study on User- Centric National Digital ID has Commenced	<p>The Malaysian Communications and Multimedia Commission (“MCMC”) announced that a study on a user-centric national digital identification (“ID”) is currently underway, having commenced on 21 November 2019.</p> <p>The 30-week study aims to recommend the implementation of a safe, secure and protected form of a Digital ID model in Malaysia which will serve as a trusted digital credential and method of authentication for Malaysians.</p> <p>The commencement of the study follows the Malaysian Cabinet’s approval to begin a comprehensive study of a National Digital ID framework. Subsequently, mandate was given to MCMC to recommend a workable National Digital ID model and further steps for the implementation of such a model.</p> <p>The study is currently supervised by the National Digital ID Task Force, which is co-chaired by the Secretary-General of the Ministry of Communications and Multimedia, Dato ‘Suriani Dato’ Ahmad, and the Malaysian Communications and Multimedia Commission Chairman Al-Ishsal Ishak.</p>	6 January 2020	<p>Press Release</p> <p>Link</p>
National 5G Task Force Report Published	<p>The National 5G Task Force was established by MCMC in November 2018 to carry out a study in order to recommend the Government of Malaysia with a holistic strategy for the deployment of the fifth generation (“5G”) mobile internet for Malaysia. The Task Force published its Report on 20 January 2020.</p>	20 January 2020	<p>Official Report (pages 89-91)</p> <p>Link</p> <p>FAQs</p> <p>Link</p>



Development	Summary	Date	Links
	<p>The Report was also formally submitted to the then Communications and Multimedia Minister, YB Gobind Singh Deo.</p> <p>Among others, the study considers the safety and security of the 5G networks to be deployed.</p> <p>The report recommended, among others:</p> <ul style="list-style-type: none">– for technical standards of 5G security to be drawn up by the Malaysian Technical Standards Forum Bhd. (a Malaysian regulatory entity designated as the Technical Standards Forum by the MCMC);– to leverage the Malaysian National Cyber Security Agency (“NACSA”) to collaborate with MCMC and any relevant private sectors (for example, private network service providers) to develop a standardised minimum-security assessment checklist that clearly defines responsibilities and standards to be upheld by the relevant parties in ensuring the deployment of secured 5G networks; and– to refer to global standards of security, namely the 3rd Generation Partnership Project (“3GPP”) Security Standard to ensure adherence of the Malaysian 5G ecosystem to stipulated network security standards. <p>The report further sets out data protection/privacy measures to be considered when any user ID data is collected during operations and maintenance exercises.</p>		



Mauritius

Contributors



Nitish Hurnaum
Partner

T: +230 211 0550
nitishhurnaum@
eversheds-sutherland.mu



Renand Pretorius
Associate

T: +230 211 0550
renandpretorius@
eversheds-sutherland.mu



Yannick Fok
Partner

T: +230 211 0550
yannickfok@
eversheds-sutherland.mu



Zaafer Raymode
Associate

T: +230 57952175
zaaferaymode@
eversheds-sutherland.mu

Development	Summary	Date	Links
<p>Global Business Licensed (“GBL”) entities are, subject to conditions, not required to register themselves as ‘Controllers’ under the Mauritius Data Protection Act 2017 (DPA 2017).</p>	<p>GBL licensed entities are mainly foreign owned entities that conduct operations outside Mauritius and are subject to the Financial Services Act 2007 (“FSA”). This is the favoured corporate vehicle for many foreign investors establishing a presence in Mauritius.</p> <p>In terms of the FSA’s regulatory framework behind these companies, all GBLs are required to be under the administrative services of a Management Company at all times.</p> <p>Given the large-scale administrative effort of all foreign owned entities being independently registered as Controllers, the Association for Trust and Management Companies raised queries with the Data Protection Office (“DPO”) and received a detailed response.</p> <p>The DPO has confirmed that a Management Company can only register on behalf of a GBL entity when the Management Company is keeping all the personal data of the GBL entity, that is when all the personal data is centralised at the Management Company.</p> <p>When this exemption is exercised, the Management Company is required to clearly indicate in its registration form, or by way of subsequent letter should registration already have been effected, that it accepts “total legal responsibility” under the DPA 2017 as</p>	31 March 2020	



Development	Summary	Date	Links
	<p>Controller of the GBL entity's activities in relation to personal information and lists all relevant details as required in the registration form for Controllers. By doing so, the Management Company, will not only have to abide with the overall provisions of the DPA 2017, but will also be liable under the DPA 2017 for each GBL entity under its management.</p> <p>However, it should be noted that, where the Management Company is not the holder of the personal information of the GBL entity under its management, the GBL entity should then register as a Controller separately.</p>		





Netherlands

Contributors



Olaf van Haperen
Partner

T: +31 6 1745 6299
olafvanhaperen@
eversheds-sutherland.nl



Marijn Rooke
Associate

T: +31 6 3026 1891
marijnrooke@
eversheds-sutherland.nl



Sarah Zadeh
Associate

T: +31 6 8188 0484
sarahzadeh@
eversheds-sutherland.nl



Robbert Santifort
Associate

T: 31 6 81880472
RobbertSantifort@
eversheds-sutherland.nl

Development	Summary	Date	Links
Dutch DPA is assessing whether Dutch car manufacturers are complying with the GDPR	<p>The Dutch Data Protection Authority ("Dutch DPA") is currently assessing if and to what extent Dutch car manufacturers are complying with the General Data Protection Regulation ("GDPR"). By doing so, the Dutch DPA hopes to gain more insight into possible GDPR violations in relation to 'connected cars', as connected cars process personal data, such as GPS-data. By letter, the Dutch DPA has asked all manufacturers of cars, commercial vehicles and trucks based in the Netherlands to inform the Dutch DPA on the personal data they process, why they process the personal data, how long they have processed it for, how they have secured the personal data and with whom they share will share the personal data.</p> <p>Based on their findings, the Dutch DPA will enter into discussions with the manufacturers. If the Dutch DPA discovers any privacy infringements, they may conduct further investigations and impose fines.</p> <p>The Dutch DPA has announced that they hope to collect and analyse all of the results of the inventory before the beginning of the summer. However, due to the recent COVID19 outbreak, the Dutch DPA has stated that if car manufacturers need more time to collect the requested information, additional time will be granted.</p>	24 March 2020	<p>Publication (in Dutch)</p> <p>Link</p>



Development	Summary	Date	Links
Dutch DPA imposed a fine on the Royal Dutch Lawn Tennis Association	<p>The Dutch DPA imposed a fine of 525,000 euros on the Royal Dutch Lawn Tennis Association (“KNLTB”) for selling the personal data of their members to third parties without a legal ground of processing.</p> <p>In 2018 the KNLTB unlawfully sold and transferred personal data of hundreds of thousands of its members to two sponsors of the KNLTB. In early 2018, the KNLTB announced in its newsletters and on its website that it would send personal data of its members to the sponsors of the KNLTB, so that the sponsors can approach the members with (tennis related) offers. In June 2018, the KNLTB provided one sponsor with personal data of 50,000 KNLTB-members and another sponsor with more than 300,000 KNLTB-members. The sponsors approached some of those KNLTB-members by mail or telephone.</p> <p>In October 2018, the Dutch DPA launched an investigation. The KNLTB stated to the Dutch DPA that they had two reasons for providing personal data to its sponsors, namely i) to create added value for the membership and ii) to obtain additional income to compensate for declining contribution income due to declining memberships. Furthermore, KNLTB stated that, based on the GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. The Dutch DPA concluded however that the sole interest in being able to cash in on personal data or to profit from them does not, in itself, qualify as a legitimate interest and that, instead, the KNLTB should have asked its members for their consent prior to the transfer of the personal data. Therefore, the Dutch DPA imposed a fine of 525,000 euros. The height of this fine was deemed appropriate by the Dutch DPA, taking into consideration the financial status of the association.</p>	3 March 2020	Publication (in Dutch) Link
Dutch DPA issued guidance for consumers regarding the purchase, lease and rental of connected cars	<p>The Dutch DPA has issued a guidance document for consumers regarding the purchase, lease and rental of connected cars. The guidance document gives consumers a number of tips when buying, renting, using and selling connected cars, for example that consumers may, under circumstances use their right of data portability after leasing or renting a connected car, and that consumers that wish to sell their connected cars should check</p>	2 March 2020	Publication (in Dutch) Link



Development	Summary	Date	Links
	prior to the sale whether they have deleted all their personal data.		
AP informs Dutch PSD2-permit holders of their GDPR-obligations	<p>The Dutch DPA is currently assessing if, and to which extent, Dutch PSD2-permit holders that are processing financial data are complying with the GDPR. The Dutch DPA hopes to find out whether these companies are aware of the privacy risks that the processing of financial data entails and whether they comply with the GDPR.</p> <p>By letter, the Dutch DPA has informed all Dutch PSD2-permit holders of the different rights and obligations as mentioned in the GDPR. The purpose of the investigation is not to impose sanctions such as fines, but if the Dutch DPA notices any violations, the Dutch DPA may conduct further investigations and impose fines.</p>	24 February 2020	Publication (in Dutch) Link
Dutch DPA published regulatory framework regarding AI and algorithms	<p>The Dutch DPA has published its regulatory framework regarding the use of artificial intelligence (“AI”) and algorithms. As described in the multi-annual document of the Dutch DPA for 2020-2023, ‘AI and algorithms’ shall be one of the three focus areas of the Dutch DPA. The regulatory framework as published by the Dutch DPA outlines the legal and regulatory framework, as well as general considerations when using AI and algorithms. The Dutch DPA has stated that they will focus on further developing its supervision on AI and algorithms in which personal data is used and will work together with other relevant parties in and outside the Netherlands.</p>	17 February 2020	Publication (in Dutch) Link
District Court ruling on the use of SyRI	<p>SyRI is a legal instrument used by the Dutch government to detect various forms of fraud, such as social security fraud and tax fraud. Several civil society interest groups, including the Dutch Section of the International Commission of Jurists and two private individuals, instituted proceedings against the State of the Netherlands as they claimed that the use of SyRI is an unacceptable violation of human rights.</p> <p>The District Court of The Hague reviewed whether the SyRI legislation is in breach of provisions of international or European law binding on all persons. The court assessed whether the SyRI legislation complies with Article 8 paragraph 2 of the European Convention on Human Rights (“ECHR”). This particular provision</p>	5 February 2020	Court Decision (in Dutch) Link



Development	Summary	Date	Links
	<p>requires the striking of a fair balance between the interests of the community as a whole, which the legislation serves, and the right of the individuals affected by the legislation to respect for their private life and home. According to Article 8 ECHR, the Netherlands has a special responsibility when applying new technologies. It must strike the right balance between the benefits such technologies bring and the violation of the right to a private life through the use of new technologies. This also applies to the use of SyRI.</p> <p>The District Court of The Hague ruled that the current legislation does not comply with Article 8(2) of the European Convention on Human Rights (ECHR), as the current legislation does not strike a fair balance, as required under the ECHR, which would warrant a sufficiently justified violation of private life. Furthermore, the legislation is insufficiently transparent and verifiable. As the current legislation concerning SyRI violates higher law, the District Court of The Hague ruled that the legislation is 'unlawful' and lacks binding effect.</p>		
District Court ruling on Article 15 GDPR	<p>The case was initiated by a claimant who claimed that the State failed to comply with his right of access request. The claimant wished to obtain copies of casefiles in which the claimant is alleged to have been involved. By granting access to those casefiles, the claimant sought to prove his innocence in another court case in which he was involved as a party.</p> <p>The legal issue in question was whether the claimant had the right to receive a copy of his casefiles. The State argued that the claim should be rejected and that the claimant had not stated or explained why the rejection of his right of access by the State was incorrect.</p> <p>As the claimant explicitly stated that he wished to obtain copies of casefiles in cases which the claimant was alleged to have been involved in order to prove his innocence in another court case, the District Court of Rotterdam considered that such an access request should not be granted, as the claimant had abused its rights based on Article 3:13 of the Dutch Civil Code.</p> <p>The purpose of the right of access as mentioned in Article 15 of the GDPR is to enable the data subject to receive a copy of their</p>	5 February 2020	<p>Court Decision (in Dutch)</p> <p>Link</p>



Development	Summary	Date	Links
	processed personal data in order to verify whether their personal data is accurate and has been processed lawfully. At the oral hearing, the claimant stated that he submitted these requests solely to prove his innocence in another court case. Thus, the District Court concluded that the purpose pursued by the claimant was not to verify the accuracy and lawfulness of his personal data, but to obtain information which he wished to use in order to provide (further) evidence in another court case. The purpose of claimant's right of access did not concern the protection of personal data. The District Court Rotterdam ruled that the claimant had abused its right of access and dismissed the claims.		
The Dutch DPA imposes sanctions on health care insurer	<p>The Dutch DPA has imposed an order subject to an additional penalty on a Dutch health insurer, CZ, for failing to comply with the GDPR. According to the investigation of the Dutch DPA, CZ had, in a number of cases, processed more medical data than necessary for the assessment of applications for reimbursement of rehabilitation care.</p> <p>CZ lodged an appeal against the AP's decision, after which the Dutch DPA and CZ made further arrangements. CZ and the Dutch DPA will hold further discussions on how to change to the current procedures in order to make them GDPR-compliant.</p>	14 February 2020	Press Release (in Dutch) Link



Poland

Contributors



Marta Gadomska-Gołab

Partner

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



Aleksandra Kunkiel-Kryńska

Partner

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



Agnieszka Sagan-Jezowska

Senior Associate

T: +48 22 50 50 730
agnieszka.sagan-jezowska@
eversheds-sutherland.pl

Development	Summary	Date	Links
List of audits of the Polish Personal Data Protection Authority (PUODO) planned in 2020	The PUODO has published a list of sectors selected for planned inspections during 2020. The sectors they plan to audit are authorities processing personal data in the Schengen Information System and the Visa Information System, BBanks - in connection with the preparation of copies and scans of identity documents of clients and potential clients and entities using the remote water meter reading system (smart meters). The full list is available at the PUODO's website.	2 January 2020	List of DP Authority's inspections planned on 2020 Link
E-mail address of employee after termination of employment may be still active, but not in use by the employer	The PUODO has officially confirmed that the e-mail address of an employee with his/her surname included may be still active even after termination of employment. An employer is able to keep the e-mail address active for example to inform its customers or contractors about new contact details with the company's representative by using an automated response. However, active usage of the personal e-mail addresses of ex-employees, for example to handle correspondence with the client, is prohibited.	17 January 2020	Statement of PUODO Link
Illegal trade of databases in banking	The PUODO notified the Polish Financial Supervision Authority (KNF) and The Polish Bank Association (ZBP) of illegal trade in the databases of banks by the bank's employees. PUODO asked for action to be taken to minimise the activity.	19 February 2020	Correspondence of PUODO with the KNF and ZBP Link



Development	Summary	Date	Links
The court upholds the administrative fine on Dolnośląski Związek Piłki Nożnej	The court upheld the administrative fine imposed on Dolnośląski Związek Piłki Nożnej for unauthorised online publishing of the personal data of football referees. The data breach was caused by the processor and went on for approximately 6 months. A fine has been imposed on the controller but the verdict is not final.	2 March 2020	Article at the UODO's official website Link
Fine for processing the fingerprints of students	The PUODO has imposed a fine on a primary school for processing the fingerprints of the students to allow access to the school canteen. The legal basis of the processing applied by the controller was consent obtained from the children's parents. There was an alternative way of access to the canteen that did not use fingerprints, but children without biometric verification permission provided from their parents were only allowed access (using the alternative way) after all children using biometric data had entered. The PUODO stated that processing biometric data of children to allow access to the canteen is a violation of the minimisation rule and is unnecessary to meet the goals of data processing. The PUODO emphasized the special character of biometric data (this being special category personal data under GDPR) and the high standards of processing that are required to justify its processing.	5 March 2020	Article at the UODO's official website Link
Guidelines on data security during remote work	The PUODO has published guidelines on general rules to ensure personal data security during remote work regarding i.a. devices, IT network access, cloud usage.	17 March 2020	Guidelines of PUODO Link



Russian Federation

Contributors



Victoria Goldman

Managing Partner

T: +7 812 363 3377

victoria.goldman@

eversheds-sutherland.ru



Ekaterina Mironova

Principal Associate

T: +7 495 662 6434

ekaterina.mironova@

eversheds-sutherland.ru



Ivan Kaisarov

Senior Associate

T: +7 812 363 3377

ivan.kaisarov@

eversheds-sutherland.ru

Development	Summary	Date	Links
<p>The government has prepared a draft decree on technically complex products and the requirement of mandatory pre-installation of Russian software</p>	<p>The draft decree includes a list of which wireless equipment is covered, including wireless equipment for domestic use having a touch screen and two or more functions; system units, stationary and portable computers, including laptops and personal computers; and TVs with digital control unit.</p> <p>A package of Russian software is to be pre-installed on all such devices, and include search engines, antivirus programs, browsers, messengers, social networks, software that provide access to the State online government services portal, instant messaging services, mail software, programs that provide free access to watch federal public television channels and radio channels, as well as a software intended for the use of national payments.</p> <p>The draft decree would also establish a procedure to compile and maintain a list of Russian software which must be pre-installed on technically complex products.</p> <p>The current proposal would exclude devices produced or brought into circulation (imported) to the Russian Federation before and until 1 July 2020.</p> <p>Currently, the draft decree is under review by the state.</p>	10 March 2020	<p>Text of the draft decree</p> <p>Link</p>



Singapore

Contributors



KK Lim

Head, Cybersecurity, Privacy and Data Protection

T: +65 6361 9307

kklim@

eversheds-harryelias.com



Janice Lee

Foreign Legal Associate

T: + 65 6361 9821

janicelee@

eversheds-harryelias.com



Valencia Soh

Associate

T: + 65 6361 9829

ValenciaSoh@

eversheds-harryelias.com

Development	Summary	Date	Links
Globalsign.in Pte Ltd was fined for data breach	Globalsign.in Pte Ltd (" Globalsign.in "), an email marketing service provider, was fined by the Personal Data Protection Commission (the "PDPC") for SGD 34,000 when its mass emailing system was accessed without authorisation in August 2017 and abused to send spam emails to 149,172 email addresses which belonged to its client's customers. The PDPC found that Globalsign.in had failed to put in place reasonable security arrangement to prevent such a cyber-attack and the company had also failed to remove personal data which was no longer necessary for legal or business purposes.	9 January 2020	PDPC decision Link
SAFRA National Service Association was fined for data breach	SAFRA National Service Association (" SAFRA ") was fined by the PDPC for SGD 10,000 for failing to put in place proper work processes for the sending of mass emails. An employee of the organisation had sent out emails attaching an Excel spreadsheet containing personal data of certain members of the organisation's shooting club to other members. SAFRA was also directed to review its internal processes, and to put in place process safeguards and written internal standard operating procedures to protect the personal data of its members.	9 January 2020	PDPC decision Link
National Healthcare Group Pte Ltd was fined for data exposure	National Healthcare Group Pte Ltd was fined by the PDPC for SGD 6,000 for failing to put in place reasonable security arrangements	9 January 2020	PDPC decision Link



Development	Summary	Date	Links
	to protect a list containing the personal data of partner doctors and members of the public from being publicly accessible online.		
PeopleSearch Pte Ltd was fined for data breach	PeopleSearch Pte Ltd (" PeopleSearch ") was fined by the PDPC for SGD 5,000 for failing to put in place reasonable security arrangements to protect the personal data of its clients. This resulted in PeopleSearch suffering a ransomware attack.	9 January 2020	PDPC decision Link
Society of Tourist Guides (Singapore) was fined for data exposure	Society of Tourist Guides (Singapore) was fined by the PDPC for SGD 20,000 for leaving its members' data exposed on its website, failing to appoint a data protection officer and failing to have in place written policies and practices necessary to ensure its compliance with the Personal Data Protection Act (the " PDPA ").	9 January 2020	PDPC decision Link
Creative Technology Ltd was fined for data breach	Creative Technology Ltd (" Creative ") was fined by the PDPC for SGD 15,000 when its online support forum (the " Forum ") was hacked sometime in mid-2018 resulting in the unauthorised disclosure of personal data of users of the Forum.	9 January 2020	PDPC decision Link
L'Oréal Singapore Pte Ltd received a warning for data exposure	L'Oréal Singapore Pte Ltd received a warning from the PDPC for exposing the personal data of seven individuals to the risk of unauthorised disclosure as a result of the company's failure to ensure appropriate testing of its website or make other security arrangements to protect the personal data.	9 January 2020	PDPC decision Link
Singapore Telecommunications Limited was fined for data exposure	Singapore Telecommunications Limited was fined by the PDPC for SGD 9,000 when it exposed the personal data of 750 of its subscribers to the risk of access by other subscribers.	11 February 2020	PDPC decision Link
SCAL Academy Pte Ltd was fined for data exposure	SCAL Academy Pte Ltd, a company which provides courses, seminars and workshops, was fined by the PDPC for SGD 15,000 for the exposure of personal data of its registrants. The personal data of the registrants were publicly accessible when an online search was done.	11 February 2020	PDPC decision Link
SPH Magazines Pte Ltd was fined for data breach	SPH Magazines Pte Ltd was fined by the PDPC for SGD 26,000 when the account of a senior moderator of its HardwareZone forum site (the " Forum ") had been accessed by an unknown hacker who used the senior moderator's credentials to retrieve personal data of members of the Forum.	11 February 2020	PDPC decision Link



Development	Summary	Date	Links
Royal Caribbean Cruises (Asia) Pte Ltd was fined for data breach	Royal Caribbean Cruises (Asia) Pte Ltd was fined by the PDPC for SGD 16,000 for failing to put in place reasonable security measures to protect the personal data stored in the company's receipt system. The company's failure resulted in its receipt system to suffer a ransomware attack affecting the personal data of about 6,000 of its customers.	11 February 2020	PDPC decision Link
NTUC Income Insurance Co-Operative Limited received a warning for data exposure	NTUC Income Insurance Co -Operative Limited was given a warning by the PDPC for failing to put in place reasonable security arrangements to prevent the unauthorised disclosure of personal data to users making enquiries through its website. 123 users received automated acknowledgement emails attached with files containing personal data belonging to 17 individuals.	11 February 2020	PDPC decision Link
AXA Insurance Pte Ltd received a warning for data breach	AXA Insurance Pte Ltd was given a warning by the PDPC for sending an email containing the personal data of 87 individuals to an unintended recipient.	11 February 2020	PDPC decision Link
Directions were imposed on Henry Park Primary School Parents' Association for data exposure	Henry Park Primary School Parents' Association (" Association ") had exposed the personal data of its parent volunteers. The personal data of parent volunteers were publicly accessible when an online search was done. The Association was directed by the PDPC to appoint a data protection officer, develop and implement internal data protection and training policies, and to put all volunteers handling personal data through data protection training.	11 February 2020	PDPC decision Link
Directions were imposed on Management Corporation Strata Title Plan No. 4375 and A Best Security Management for data breach	The PDPC found that Management Corporation Strata Title Plan No. 4375 (" MCST 4375 ") and A Best Security Management (" ABSM ") had failed to put in place reasonable security arrangements to prevent the unauthorised disclosure of CCTV footage of an individual injured by a falling glass door at Alexandra Central Mall (the " CCTV Footage "). The CCTV Footage was posted onto the video-sharing website YouTube. MCST 4375 was directed by the PDPC to implement policies necessary for the protection of personal data in its possession and/or under its control, put in place reasonable security arrangements for the protection of personal data, conduct training to ensure that its staff are aware of and will comply with, the requirements of the PDPA.	19 March 2020	PDPC decision Link



Development	Summary	Date	Links
	ABSM was directed by the PDPC to put in place reasonable security arrangements including policies necessary for the protection of personal data in its possession and/or under its control.		
Management Corporation Strata Title Plan No. 3593 was fined, and directions were imposed on New-E Security Pte Ltd for data breach	<p>The PDPC found that Management Corporation Strata Title Plan No. 3593 (“MCST 3593”) and New-E Security Pte Ltd (“New-E”) had failed to put in place reasonable security arrangements to prevent the unauthorised disclosure of CCTV footage of a common property at Marina Bay Residences (the “CCTV Footage”). The CCTV Footage had captured images of identifiable individuals who had passed through the common property.</p> <p>For the violation of the PDPA, the PDPC imposed a fine of SGD 5,000 on MCST 3593 and New-E was directed to put in place a data protection policy and internal guidelines, including procedures for proper management and access control in respect of CCTV footage.</p>	19 March 2020	PDPC decision Link
SSA Group International Pte Ltd received a warning for data breach	SSA Group International Pte Ltd was given a warning by the PDPC for failing to put in place reasonable security arrangements to prevent the unauthorised access of 53 individuals’ course registration information which were publicly available via its webpage.	19 March 2020	PDPC Case Link
Memorandum of Understanding between the Personal Data Protection Commission and Office of the Australian Information Commissioner	<p>A Memorandum of Understanding (the “MOU”) between the PDPC and the Office of the Australian Information Commissioner (the “OAIC”) was signed.</p> <p>Under the MOU, the PDPC and the OAIC will jointly promote the APEC Cross Border Privacy Rules (the “CBPR”) System to improve awareness and participation, as well as encourage industries to adopt the CBPR System.</p> <p>The MOU would also enable Singapore and Australia to develop compatible and interoperable data transfer mechanisms which will allow businesses operating in both countries to transfer personal data more seamlessly across borders with the assurance that they meet the requisite regulations.</p>	25 March 2020	PDPC Press Release Link



Contributors

South Africa



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
Commencement of the Protection of Personal Information Act – 1 April 2020	<p>South African President Cyril Ramaphosa has received a request from the Information Regulator Chairperson to declare that the remaining provisions of the Protection of Personal Information Act (POPIA) commence on 1 April 2020.</p> <p>Given the global COVID-19 pandemic, it seems inevitable that this date will be postponed but it is not clear by how long. When the President acts on the Information Regulator's request, organisations will have a 12 month grace period to comply.</p> <p>To date, only certain sections of POPIA are in effect, such as those provisions concerning the establishment of the Information Regulator and the way in which regulations may be promulgated.</p> <p>Once POPIA is in full effect, it will regulate the way in which public and private entities process personal information of both natural and juristic persons.</p> <p>Non-compliance with POPIA may result in administrative fines of up to R10 million, imprisonment, civil damages and most importantly, reputational harm. It is important that all businesses ensure compliance with POPIA prior to its commencement.</p>	10 March 2020	



Spain

Contributors



Juan Díaz
Managing Partner

T: +34 91 429 43 33
jdiaz@
eversheds.es



Vincente Arias Máiz
Partner

T: +34 91 429 43 33
varias@
eversheds.es



Celia Bouzas González
Senior Associate

T: 34 91 429 43 33
cbouzas@
eversheds-sutherland.es

Development	Summary	Date	Links
The Spanish Data Protection Agency (AEPD) has issued a resolution that creates a precedent on the right to data portability	<p>This resolution arises from a complaint filed with the AEPD by a user who exercised his right to portability with a telecommunications company and was not satisfied with the data provided, since they only wanted to allow the portability of data that had been directly provided by the applicant: name, surname, ID, telephone, address, email and bank details. The citizen claimed that he should have been provided with certain data listed in the privacy policy and resulting from the use or development of the service such as products or services, consumption, traffic, website visits and location.</p> <p>The resolution considered that the portability of the data was carried out incompletely and that the controller should have provided some of the data requested by the user. This decision extends the content of the right of portability to certain data resulting from the use of the service such as consumption, traffic and location, but does not include data on visits to websites. Similarly, the resolution excludes from this right the access and portability of data referred to in the law 25/2007 on data retention for the purpose of investigating crimes.</p>	5 February 2020	Resolution on the official website of the AEPD. Link



Development	Summary	Date	Links
The AEPD publishes a guide to adapt products and services using Artificial Intelligence to the GDPR	<p>The guide, which is addressed to controllers who incorporate AI components in their processing, as well as to developers and managers supporting such processing, begins by introducing the relationship between AI and data protection, since an AI element could be processing personal data at different stages of its life cycle and, consequently, would have to comply with the obligations set forth in the GDPR.</p> <p>The guide goes on to review the different relationships that may exist between the controller of personal data and the third parties that could be hired to perform tasks. The guide also sets out the conditions that these technologies must fulfil in order to guarantee and demonstrate that the processing carried out is in accordance with the GDPR. These include aspects such as legitimacy for processing, information, exercise of rights and automated decision making. The document also addresses the risk management of a processing operation for rights and freedoms as part of the concept of active responsibility established in the GDPR, focusing on aspects such as accuracy, minimization of data, impact assessment and analysis of the proportionality of the processing, among others. Finally, it analyses the possibility that the use of AI-based technologies implies international data transfers.</p> <p>The guide concludes that placing technology that uses AI on the market requires quality and privacy guarantees to be applied. The guide also mentions that compliance with the provisions of the GDPR requires a certain level of maturity of the AI models so that the adequacy of the processing and the existence of measures to manage its risks can be objectively determined.</p>	13 February 2020	<p>Guide to adapt products and services using Artificial intelligence to GDPR</p> <p>Link</p>



Sweden

Contributors



Torbjörn Lindmark
Partner

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



Josefine Karlsson
Senior Associate

T: +46 7 33 12 28 81
josefinekarlsson@
eversheds-sutherland.se

Development	Summary	Date	Links
Swedish DPA: audits have been initiated based on Clearview AI potential business with Swedish authorities	The Swedish Data Protection Authority (the "DPA") initiated audits of Swedish authorities to determine whether Swedish authorities use facial recognition technology provided by Clearview AI.	6 March 2020	Press Statement (in Swedish) Link
Swedish DPA: a report has been published on data breach notifications made during 2019	<p>The Swedish DPA issued a report on data breach notifications made in 2019. The report shows, among other things:</p> <ul style="list-style-type: none"> – a total of 4,800 notifications were made; – the public sector is in the top of number of notifications made, and both government authorities and the health care sector reported twice as many data breaches compared to 2018; and – the most common incident is emails or postal mails sent to the wrong recipient. 	9 March 2020	Press Statement (in Swedish) Link Report (in Swedish) Link
Swedish DPA: an audit of Swedish police has been initiated	<p>Swedish police have, on several occasions during the period November 2019 to January 2020, provided excerpts from criminal records that either included too much or too little information.</p> <p>A total number of 450 excerpts were affected and the data subjects concerned have been informed. The police have stated that the reason for the breach is a change of IT platform.</p>	26 February 2020	Press Statement (in Swedish) Link



Development	Summary	Date	Links
	The Swedish DPA initiated an audit to determine, among other things, if measures taken to mitigate the risk of the breach and to prevent future breaches are sufficient.		
Swedish DPA: Digital service for data breach notifications	The Swedish DPA launched an electronic means for data breach notification.	12 March 2020	Press Statement (in Swedish) Link Data Breach notification service (in Swedish) Link
Swedish DPA: Administrative fine of MSEK 75 to Google	<p>The Swedish DPA initiated a follow-up audit of Google due to information indicating that Google did not fully comply with the previously issued order to delete certain search results.</p> <p>Following this follow-up audit, it was clear that Google had not followed the previous order and the DPA therefore issued a fine of MSEK 75 (approx. Euro 7.5 million).</p> <p>Additionally, the Swedish DPA issued a cease and desist from Google's practice of providing information to site-owners in relation to requests to delist search results. The Swedish DPA finds that this practice discourages people to use the delisting function and also provides misleading information.</p>	11 March 2020	Press Statement Link
Swedish DPA: Annual report from the Swedish Data Protection Authority	<p>The Swedish DPA issued its annual report in which, among other things, the following was presented:</p> <ul style="list-style-type: none"> – as part of its supervisory work, 60 new matters were initiated; – 6,400 written questions were sent from private or public businesses of which 900 were of a complicated nature; – 4,000 complaints from individuals were received; – 2,300 notifications on data protection officers; and – 500 applications on a permit for CCTV. 	21 February 2020	Press Statement (in Swedish) Link Annual Report (in Swedish) Link



Development	Summary	Date	Links
Swedish DPA: Report is issued on complaints in relation to search engines for personal information	<p>The Swedish DPA issued a report on the most frequent complaint received from the public, namely in relation to various search engines where extensive personal data is published.</p> <p>The report states that almost every fifth complaint received is in relation to this kind of service. The aim of the report is to provide an in depth understanding of the risks, concerns and consequences that the public connect to search engines for personal data.</p> <p>It can be noted that these companies provide their services based on what is referred to as a voluntary publication authorisation.</p>	28 January 2020	<p>Press Statement (in Swedish) Link</p> <p>Report (in Swedish) Link</p>





United Arab Emirates

Contributors



Geraldine Ahern
Partner

T: +97 1 24 94 36 32
geraldineahern@
eversheds-sutherland.com



Erica Werneman Root
Senior Associate

T: +97 1 43 89 70 34
ericawernemanroot@
eversheds-sutherland.com

Development	Summary	Date	Links
DIFC - The new data protection law is nearing publication	In June 2019, the DIFC published a consultation to fully update the existing data protection law and bring it in line with international best practice. The updated law will expand and clarify issues around: accountability, jurisdiction, data breach notification, prior consultation, data protection officer appointments, consent, administrative requirements and sanctions/enforcement. Importantly, the updated law will also address issues around data subjects' rights in the context of emerging technologies. We expect that the new law will be published in March or April 2020 and the Commissioner has set a target date of 1 July 2020 for enactment.	1 April 2020	



United Kingdom

Contributors



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



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

Development	Summary	Date	Links
DMA announces data protection as the main priority in Brexit negotiations	The UK's Data & Marketing Association (" DMA ") announced that data protection would be one of the most important issues on the agenda of Brexit negotiations. The free-flow of data between the UK and EU is intrinsic to the functionality and operation of many businesses. To support UK government and EU intend to agree an 'adequacy agreement' which will impose a mutual obligation in both jurisdictions to respect individuals' rights in relation to their personal data. The agreement will facilitate the processing, storage and use of personal data within each other's jurisdiction.	9 January 2020	Press release Link
ICO calls for views on the processing of personal data relating to criminal convictions	<p>The Information Commissioner's Officer ("ICO") has published a survey to assess whether there are any deficits in data controllers' knowledge of the data protection requirements under Article 10 GDPR. Under Article 10, organisations can process personal data relating to criminal convictions and offences, or related security measures, for certain reasons, for example to safeguard vulnerable individuals.</p> <p>The ICO is calling for controllers and/or processors of Article 10 data to participate and complete the survey by Friday 28 February 2020.</p>	20 January 2020	Press release Link Survey Link
ICO publishes final Age Appropriate Design Code	<p>The ICO has published its final Code of Practice to protect children's privacy – the Age Appropriate Design Code.</p> <p>The code contains 15 standards, rooted in the GDPR, which online service providers should meet to protect a child's right to privacy. The standards do not prohibit any actions or prescribe any obligations, however if followed, the standards will enable online services to provide built-in protection to allow children to explore,</p>	21 January 2020	Code Link



Development	Summary	Date	Links
	play and learn online without putting them at risk of any online harm.		
ICO amends guidance on timescales for complying with DSARs when clarification is sought	<p>The ICO has amended its GDPR guidance, changing the position on timescales when the controller requests clarification from the data subject.</p> <p>The time limit is not paused while the controller waits for a response to its request. This is a divergence from previous guidance issued by the ICO.</p> <p>This new position is also reflected in the draft DSAR issued for consultation (see above).</p>	22 January 2020	<p>Updated guidance</p> <p>Link</p>
ICO responds to Metropolitan Police Service's announcement on their future use of LFR	<p>Following its investigation into how the police force uses live facial recognition technology ("LFR") in public places, the ICO has published an Opinion which found that, although there was public support for the use of LFR by the police, major improvements to how the police permit and deploy LFR were required if the police wish to maintain public trust and address privacy concerns.</p> <p>The Metropolitan Police Service ("MPS") responded by incorporating the ICO's advice from the Opinion into the future planning and preparation of LFR use. MPS has made a commitment to comply with data protection legislation, and reduce individuals' invasion of privacy.</p> <p>The ICO responded in a statement to MPS's assurances that it will review each future deployment of LFR. In the statement, the ICO reiterated that LFR is still a top priority and that the ICO is continuing to conduct several investigations. The ICO will produce further reports of LFR use by the private sector later this year.</p>	24 January 2020	<p>ICO statement</p> <p>Link</p>
NCSC publishes design guidelines for high assurance products	<p>The National Cyber Security Centre ("NCSC") has published design guidelines for high assurance products for users and developers about products and systems whose purpose is to protect against elevated cyber threats (that is, threats that aim to circumvent mass-produced cyber security tools). The principles are designed for use where NCSC "certified assisted products" evaluation is not appropriate (CAPS high grade assessment being</p>	6 February 2020	<p>Guidelines</p> <p>Link</p>



Development	Summary	Date	Links
	an independent assessment by the NCSC of primarily cryptographic products).		
CDEI publishes final report on online targeting	<p>The Centre for Data Ethics and Innovation (“CDEI”) published a final report following its review of online targeting. Online targeting systems are those which promote content on social media platforms, recommend videos, and customise search engine results.</p> <p>CDEI revealed that internet users understand the advantages of online targeting – namely, it personalises online experiences, and enables convenience. However, users also expressed concern with the lack of accountability by organisations for the damage that targeting systems can cause to vulnerable individuals.</p> <p>The report specifies three sets of recommendations including:</p> <ul style="list-style-type: none"> – Accountability – the government is currently developing a regulatory regime which is intended to manage the threat of online harms by holding organisations accountable for their use of targeting systems; – Transparency – CDEI encourages online targeting systems to be more transparent so that internet users can appreciate the effects of such systems. This requires system operators to make data processed for sensitive areas publicly accessible; and – User empowerment – the new regime should provide users with more information and greater control including the incorporation of a ‘fairness by design’ duty for online platforms. 	4 February 2020	Final report Link
Private Member’s Bill for moratorium on and review of the use of AFR technology in public spaces	A new Private Member’s Bill has been introduced in the House of Lords to prohibit the use of automated facial recognition (“ AFR ”) technology in public places, and to make such surveillance a criminal offence. The Bill also requires the government to conduct an annual review such use of AFR technology, including an examination of equality and human rights implications, data protection implications, quality and accuracy of technology, and adequacy of the regulatory regime governing data sharing and processing.	4 February 2020	Private Member’s Bill Link



Development	Summary	Date	Links
DCMS publishes outcome of consultation on regulatory proposals on consumer Internet of Things security	<p>Following its 2019 consultation on regulatory proposals on consumer Internet of Things (“IoT”) security, the Government has concluded that it will implement legislation that mandates the following three principles:</p> <ul style="list-style-type: none"> – all IoT device passwords to be unique and not resettable to any universal factory default value; – each manufacturer to provide a public point of contact as part of a vulnerability disclosure policy to enable security researchers and others to report issues; and – each manufacturer to explicitly state the minimum length of time for which the product will receive security updates. <p>The Government has described these requirements as the “first practical step towards more secure devices”. The Government will now carry out further stakeholder engagement to develop this first phase stage of regulation, in particular to consider how those selling into the UK can best communicate security information to consumers at the point of sale whilst ensuring minimum disruption to the supply chain.</p> <p>By way of background, in October 2018 the Government published a Code of Practice for IoT Security which provided guidance for consumers on how they can help set up and manage their smart devices to improve their safety and protect their personal information. In February 2019, the European Telecommunications Standards Institute’s Technical Committee on Cyber-Security issued the ETSI industry standard technical specification 103 645 on internet connected consumer devices, which was based on the Government’s Code of Practice.</p>	3 February 2020	Response to consultation Link
Standards in Public Life Committee published a report on AI in the public sector	<p>The Committee on Standards in Public Life has released a report and accompanying recommendations on artificial intelligence (“AI”) and public standards.</p> <p>The report acknowledges that AI is capable of fundamentally altering how the public sector functions and provides services. However, the publication also recognises the problems with an increased use of AI. To address these issues, the report recommends several principles to follow including the</p>	10 February 2020	Report and recommendations Link



Development	Summary	Date	Links
	implementation of ethical standards for the public sector to use, and recommendations to providers of public services, both public and private, to help them develop effective risk-based governance for AI – including measures focusing on legal and legitimate AI, system design, and diversity, setting responsibility, internal and external oversight, monitoring and evaluation, appeal and redress, and training and education.		
DCMS publishes initial consultation response announcing Ofcom as the UK's regulator of Online Harms	<p>The Department for Digital, Culture, Media & Sport ("DCMS") and the Home Office issued an initial joint statement in response to the Online Harms White Paper consultation, which ran from 8 April 2019 to 1 July 2019.</p> <p>The initial response confirms that Ofcom will be appointed as the UK regulator because it is deemed to have the necessary 'organisational experience, robustness, and experience of delivering challenging, high-profile remits across a range of sectors'.</p> <p>According to the statement, the regulatory framework proposed by the Online Harms White Paper will only be applicable to about 5% of UK businesses – the duty of care introduced by the new framework will only apply to companies that facilitate the sharing of user generated content, for example through comments, forums or video sharing. The statement confirms: <i>"To be in scope, a business would have to operate its own website with the functionality to enable sharing of user-generated content, or user interactions"</i>. In addition, the departments confirm that guidance will be provided by the regulator to help businesses understand whether or not the services they provide or functionality contained on their website would fall into the scope of the regulation. The departments also acknowledge that increased levels of protection for children must be reflected in any regulatory framework.</p>	12 February 2020	Press release Link
ICO consults on the draft AI auditing framework guidance for organisations	<p>The ICO launched a consultation on its draft AI auditing framework. The framework aims to provide guidance on how the data protection legislation impacts AI. The ICO intends to produce comprehensive guidance on how organisations can introduce operational and technical measures to mitigate the risks that AI poses. The closing date for submitting responses is 1 April 2020.</p>	19 February 2020	ICO announcement Link



Development	Summary	Date	Links
Data protection and Brexit update	<p>UK Government report on its future relationship with the EU (28 February 2020): On 28 February, the UK Government published a report on the UK's approach to its future relationship with the EU. The report highlights that the UK will have an independent policy on data protection at the end of the transition period but will remain committed to high data protection standards. The report also sets out that the UK will seek adequacy decisions from the EU before the end of the transition period to ensure that the free flow of personal data from the EU and EEA states to the UK is maintained. The report also states the Government's intention to seek "<i>appropriate arrangements</i>" to allow continued cooperation between the ICO and the EU Member State's data protection authorities.</p> <p>EDPS Opinion on EU-UK future data protection relationship (24 February 2020): On 24 February, the European Data Protection Supervisor ("EDPS") has published an Opinion on the opening of negotiations for a new partnership with the UK. The EDPS supports and welcomes the Commission's objective to conclude a comprehensive partnership with the UK. The Opinion emphasises the importance of involving the EDPB in any adequacy assessment and the importance of the Commission clearly defining the scope of any adequacy decision. The EDPS recommends that the EU prepares for all eventualities including "<i>where the adequacy decision(s) could not be adopted within the transition period, where no adequacy decision would be adopted at all, or where it would be adopted only in relation to some areas</i>" and reminds the Commission that if it were to adopt an adequacy decision, "<i>it must subsequently monitor developments in the UK and, if it considers that the UK no longer provides an adequate level of protection, it can repeal, amend or suspend its decision...</i>".</p> <p>Council of the EU negotiations mandate (22 February 2020): In the addendum to its decision, dated 25 February, authorising the opening of negotiations with the United Kingdom of Great Britain and Northern Ireland for a new partnership agreement, the Council of the European Union expressed the following (page 6): "<i>In view of the importance of data flows, the envisaged partnership should affirm the Parties' commitment to ensuring a high level of personal data protection, and fully</i></p>	21-28 February 2020	<p>UK Government report Link</p> <p>EDPS Opinion Link</p> <p>Council of EU Addendum Link</p> <p>European Parliament resolution Link</p>



Development	Summary	Date	Links
	<p><i>respect the Union's personal data protection rules, including the Union's decision-making process as regards adequacy decisions. The adoption by the Union of adequacy decisions, if the applicable conditions are met, should be a factor for fostering cooperation and exchange of information. It is also a condition, where necessary, to achieve the high level of ambition on law enforcement and judicial cooperation in criminal matters as envisaged in section 2 of Part III".</i> The addendum also contained commentary on the importance of addressing data protection rules in the contexts of digital trade (page 16) and law enforcement and judicial cooperation in criminal matters (pages 33-34).</p> <p>European Parliament (EP) proposed UK/EU negotiation mandate (12 February 2020): Interestingly, only a couple of weeks prior, the European Parliament had highlighted a number of specific areas for the European Commission to consider in relation to any UK adequacy assessment, in its proposed UK/EU negotiation mandate (paragraphs 32-34). The Parliament instructed the European Commission to “carefully assess” the UK’s data protection legal framework and ensure the UK has resolved the following prior to considering UK data protection law adequate in line with EU law:</p> <ul style="list-style-type: none"> – immigration exemption in DPA 2018 (Schedule 2 Part 1 paragraph 4); – UK’s legal framework on the retention of electronic telecommunications data; and – UK’s legal framework on national security and processing by law enforcement authorities, particularly mass surveillance programmes which may not be adequate when considering <i>Schrems</i> case and ECHR case law. 		
The FCA issues statement following data breach	<p>The Financial Conduct Authority (“FCA”) announced that underlying confidential information may have been accessible following the publication of its response to a Freedom of Information Act request. The response detailed the number and nature of new complaints made against the FCA but in some cases, this included personal data such as names, addresses and telephone numbers of data subjects.</p>	25 February 2020	<p>Press release</p> <p>Link</p>



Development	Summary	Date	Links
	Following the breach, the FCA removed the relevant data and carried out a full review to identify the extent of any information that may have been accessible. The FCA confirmed that no financial, payment card, passport or other identity information were included and that the FCA has reported the breach to the ICO.		
ICO publishes guidance on developing Codes of Conduct and Certification schemes	<p>The ICO has published guidance for organisations who are developing Codes of Conduct or Certification schemes under the GDPR.</p> <p>Trade associations and other representative bodies are able to develop codes of conduct, identifying and addressing data protection issues that are important to their members. The ICO are encouraging this as a method of establishing sector-specific guidelines to aid compliance with the GDPR. Organisations can submit their proposals for these schemes to the ICO for approval. Once approved, other organisations can sign-up to a code of conduct, allowing them to ensure they are following the rules that developed for their sector.</p> <p>Certification enables organisations to demonstrate compliance with the GDPR and by allowing them to show they have appropriate technical and organisational measures to ensure data security. Certification can apply either generally to a variety of matters or to one specific issue. An organisation will be assessed by the accredited certification body for a scheme and, if successful, will be issued with a data protection certificate, seal or mark which is relevant to that scheme.</p>	28 February 2020	<p>ICO statement Link</p> <p>Codes of conduct: detailed guidance Link</p> <p>Certification: detailed guidance Link</p>
National Cyber Security Centre publishes guidance on cyber protection for 'smart' security cameras	<p>The National Cyber Security Centre ("NCSC") has published guidance explaining how smart security cameras and baby monitors can be protected from cyber-attacks.</p> <p>The guidance explains how smart cameras connect to the internet using home Wi-Fi enabling a live camera feed, and that it is possible for them to be accessed by unauthorised users. The NCSC recommends four steps to ensure that the device is safe, including changing the default password to a secure one, regularly updating the camera's software/firmware, checking router settings and disabling the feature(s) that enable remote viewing camera footage via the internet UPnP and port</p>	3 March 2020	<p>Guidance Link</p>



Development	Summary	Date	Links
	forwarding, and disabling the feature that lets you remotely view camera footage via the internet if this is a feature that is not used.		
Verbal disclosure does not constitute 'processing' of personal data under DPA 1998	<p>In Scott v LGBT Foundation Ltd [2020] EWHC 483 (QB), the court considered whether a charity had breached the Data Protection Act 1998 ("DPA 1998") in disclosing personal data about the claimant in a telephone conversation with his GP.</p> <p>The court held that there had been no breach because the disclosure had been made verbally – it did not amount to "processing" for the purposes of the DPA 1998 as it had not been recorded in either electronic or manual form. Further, the court found that if the disclosure had amounted to processing, then it would have been lawful on the grounds of it being necessary to protect the data subject's vital interests.</p>	5 March 2020	Judgment Link
UK and Australia data protection authorities sign a memorandum of understanding	<p>The Office of the Australian Information Commissioner and the ICO have signed a memorandum of understanding for cooperation in the regulation of laws protecting personal data and upholding information rights. The MoU captures the intention of both authorities to better protect personal data through:</p> <ul style="list-style-type: none"> (i) sharing experience, expertise and ways or working; (ii) cooperating on specific projects and investigations; and (iii) sharing intelligence and information to support their work. 	5 March 2020	ICO blog post Link
Government establishes Digital Markets Taskforce to advise on delivery of digital markets objectives	<p>In a move reflecting global efforts by competition and anti-trust regulators to adapt to digital markets, the government announced it would be establishing a new Digital Markets Taskforce to sit within the Competition and Markets Authority ("CMA"), and comprise officials from the CMA, Ofcom and the ICO.</p> <p>The aim of the taskforce is to provide the government with expert advice on the functions, processes and powers needed to deliver on the government's objectives in digital markets in a proportionate and efficient way.</p> <p>The taskforce will operate until September 2020 when it will deliver a report on its recommendations. The report will contain recommendations and advice on a number of matters,</p>	12 March 2020	Government statement Link



Development	Summary	Date	Links
	including: a potential methodology to designate digital platforms with “strategic market status” and whether intervention to promote competition is necessary and justified in relation to platforms/activities that do not fall within that remit; the form that a code of conduct to promote competition could take and the content of such code; the associated powers and processes needed to operate and enforce any code(s); whether there is a case for remedies relating to data access and interoperability outside of search and social media markets; advice on the pro-competitive regime’s interplay with existing regulatory regimes including those governing economic growth and innovation, privacy, data protection, and intellectual property rights; and where international cooperation between a pro-competitive regime and other jurisdictions and multilateral fora would be most valuable or necessary.		
FCA publishes industry insights into cyber resilience	<p>In 2017, the FCA brought together the Cyber Coordination Groups (“CCG”), comprising over 175 firms across different financial sectors to share information and ideas from their cyber experiences. The CCGs have shared their knowledge of their common experiences in their latest insights paper, which covers: cyber risk; identity and access management; third parties and supply chain; and malicious emails.</p> <p>The paper identifies the following as emerging risks and future trends: Development and Security in Operations (DevSecOps) which integrates security by design into the development operations processes by ensuring security is an integrated consideration at each stage of the development process; Cloud security risk including reduced visibility and control of risks, insecure or misconfigured cloud instances/interfaces, concentration risk, insider risk (e.g. abuse of trust or of privileged access) to manipulate and or gain access to sensitive data and services; and payment systems security (including vulnerabilities in core systems such as payment messaging and transaction authorisation).</p>	13 March 2020	CCG insights Link
Court of Appeal sheds light on application of legal privilege	In Dawson-Damer v Taylor Wessing [2020] EWCA Civ 352 , the Court of Appeal allowed appeals from both sides against a High Court judgment that a law firm’s paper files constituted a “relevant filing system” under the DPA 1998 and that the legal	11 March 2020	Judgment Link



Development	Summary	Date	Links
exemption and relevant filing system under DPA 1998	<p>professional privilege (“LPP”) exemption could apply to documents in scope of a subject access request.</p> <p>The case involved subject access requests which were made to the solicitors of the trustees of a foreign trust. The High Court had found that “joint privilege” applied but the Court of Appeal disagreed and held that this was a matter of domestic procedure and evidence rather than one of local trust law.</p> <p>The Court of Appeal also considered whether the paper files held by the law firm constituted a relevant filing system under the DPA 1998. It held that the documents were not readily retrievable according to a specific criteria – the Court cited the ICO’s “temp test” in coming to its conclusion</p>		
DCMS publishes UK data protection explanatory framework to assist European Commission adequacy assessment	<p>The DCMS has published a pack of explanatory material, which provides an overview of the UK’s legal framework underpinning data protection standards in order to assist the European Commission in conducting its assessment of the UK for adequacy under Article 45 GDPR and Article 36 of the Law Enforcement Directive, to ensure the continued free flow of personal data between the EU, the UK and Gibraltar.</p> <p>The documents aim to illustrate the UK’s “long and proud tradition of defending privacy rights” by emphasising a number of features of its data protection legal landscape, including: the ICO’s role as a reliable, experienced and capable independent regulator; robust principles; clear grounds limiting when processing of personal data is lawful; and effective and enforceable rights of individuals.</p> <p>The covering note ends by confirming that the “UK stands ready to offer further clarifications throughout the assessment process and looks forward to an open dialogue with the Commission”.</p>	13 March 2020	<p>Framework and press release</p> <p>Link</p>
The SCC and the ICO publish a new template DPIA and updated guidance on DPIAs for surveillance cameras	<p>The Surveillance Camera Commissioner (“SCC”) and the ICO have released updated guidance specifically for the use of surveillance cameras. The update includes a new template DPIA with associated guidance notes, and aims to provide an approach in line with the updated data protection requirements contained</p>	18 March 2020	<p>Press release</p> <p>Link</p> <p>Template DPIA and guidance</p> <p>Link</p>



Development	Summary	Date	Links
	<p>in the Data Protection Act 2018, the GDPR and the Protection of Freedoms Act 2012.</p> <p>It is hoped this joint effort between the SCC and the ICO will ensure surveillance camera systems are implemented for the protection of citizens rather than spying, and that public trust in the use of such systems will be strengthened.</p>		
Task Force for Relations with the United Kingdom publishes draft text of Agreement on the New Partnership with the United Kingdom – affirming commitment to ensuring high level of data protection	<p>The Task Force for Relations with the United Kingdom of the European Commission published a Draft Text of the Agreement on the New Partnership with the United Kingdom. The draft agreement documents the parties' commitment to ensuring a high level of data protection and collaboration to promote high international standards. In addition, the Draft Agreement highlights that the parties are also committed to ensuring cross-border data flows to facilitate trade in the digital economy. Moreover, the Draft Agreement outlines that each party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data.</p>	18 March 2020	<p>Press release</p> <p>Link</p>
Online advertising call for evidence: government extends deadline	<p>The DCMS has extended the deadline for submissions to the Call for Evidence from Monday 23 March 2020 to Monday 6 April 2020. This Call for Evidence forms the first pillar of work in DCMS's review of the regulation of online advertising. This review is intended to supplement various ongoing reviews of the sector by the CMA, the Centre for Data Ethics and Innovation and the ICO.</p>	18 March 2020	<p>Govt release</p> <p>Link</p>
UK Government releases statistics on cybersecurity breaches	<p>The DCMS released its annual Cyber Security Breaches Survey 2020. The survey undertook a quantitative and qualitative study of UK business and charities to aid their understanding on the nature and significance of cybersecurity threats. In summary, the Survey highlighted the following findings:</p> <ul style="list-style-type: none"> • The extent of cybersecurity threats has not diminished and in fact, have evolved and gained frequency. • Organisations have become increasingly resilient to breaches and are less likely to report negative impacts from breaches and more likely to recover faster. 	26 March 2020	<p>Survey</p> <p>Link</p>



Development	Summary	Date	Links
	<ul style="list-style-type: none"> In the last five years, businesses and charities have shown greater board engagement in cybersecurity and taken steps to identify and manage cyber risks. Key growth areas for organisations were identified and comprise audits, cyber insurance, supplier risks and breach reporting. <p>The survey further highlights that 46% of businesses and 26% of charities have reported cyber security breaches in the last year, with the annual average cost of cyber security breaches estimated at £3,230. Of the businesses targeted by cyber-attacks, 39% were negatively impacted notably through business disruption.</p>		
Supreme Court finds UK Home Office sharing of personal data with US breached Part 3 of DPA 2018	<p>In Elgizouli (Appellant) v Secretary of State for the Home Department (Respondent) [2020] UKSC 10, the appellant's son was alleged to have been part of a terrorist group operating in Syria, and involved in the murder of US and British citizens. In June 2015, the US made a mutual legal assistance ("MLA") request to the UK in connection with the activities of the group. The UK Home Secretary requested an assurance that the information would not be used directly or indirectly in a prosecution that could lead to the imposition of the death penalty, which the US refused to provide. In June 2018, the Home Secretary agreed to provide the information without requiring any assurance. The appellant challenged this decision via judicial review.</p> <p>The Supreme Court considered whether sections 73 to 76 of the DPA 2018 prevented the Home Secretary from providing MLA (in this case, a transfer of personal data) to the US, which would facilitate the imposition of the death penalty on the relevant individual.</p> <p>The Supreme Court considered the following questions:</p> <ol style="list-style-type: none"> whether the common law has evolved in such a way to render it unlawful for the Home Secretary to provide MLA to supply evidence to a foreign state that will facilitate the imposition of the death penalty on the individual in respect of whom the evidence is sought; and 	26 March 2020	<p>Supreme Court case webpage Link</p> <p>Press summary Link</p> <p>Judgment Link</p>



Development	Summary	Date	Links
	<p>2. whether it is lawful under Part 3 of the DPA 2018 for law enforcement authorities in the UK to transfer personal data to law enforcement authorities abroad for use in capital criminal proceedings.</p> <p>The Supreme Court concluded that the answer to the first question was “no”.</p> <p>However, the court allowed the appeal in respect of the second question – unanimously finding that the Home Secretary had not properly considered his duties under the DPA 2018 in deciding to provide MLA to the US. The court held that since there was no adequacy decision or appropriate safeguards applicable to the transfer, that it would need to meet the special circumstances requirement detailed in section 76 DPA 2018, and this was not met as the transfer was not strictly <i>necessary</i> for any of the five purposes set out in the section.</p>		



United States

Contributors



Michael Bahar
Partner

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



Pooja Kohli
Litigation Specialist

T: +1 212 389 5037
PoojaKohli@
eversheds-sutherland.com



Paul McCulloch-Otero
Counsel

T: +1.212.301.6604
paulmcculloch@
eversheds-sutherland.com



Sarah Paul
Partner

T: +1.212.301.6587
sarahpaul@
eversheds-sutherland.com

Development	Summary	Date	Links
Proposed CCPA regulations receive second modification	<p>On March 11, 2020, the California Attorney General released a second set of revised draft regulations under the California Consumer Privacy Act (CCPA). The key changes include:</p> <ol style="list-style-type: none"> 1. Categories of sources and purposes: The requirement for companies to identify in their privacy policies the categories of sources from which personal information (PI) is collected and the business or commercial purpose for which PI is collected or sold has been restored from the original draft regulations issued in October. However, the categories of sources and purposes need not be specified for each category of PI identified. In addition, the categories of third parties with whom the business shares PI remains deleted. Due to the fact that this requirement is being re-added to the draft regulations after prior deletion, we expect it to appear in the final regulations. 2. Financial incentives definition expanded: The definition of “financial incentive” appears to have been significantly broadened, potentially expanding the situations in which notice of the material terms of a financial incentive is required. Rather than defining a “financial incentive” as a program, benefit or offering made “as compensation” for the disclosure, deletion or sale of PI, the definition now includes any program, benefit or offering “related to the collection, 	<p>Amendments to CCPA Draft Regulations: 1 April 2020</p> <p>Comment period closes: 27 March 2020</p>	<p>CCPA Draft Regulations Link</p> <p>Legal Alert: Proposed CCPA regulations receive second modification Link</p>



Development	Summary	Date	Links
	<p>retention, or sale of personal information.” This change may encompass any programs and benefits that are connected to collection of personal information, like providing coupons or discounts as part of customer loyalty rewards programs.</p> <ol style="list-style-type: none"> Particularity of responses to a request to know: The prohibition on disclosing social security numbers and similarly sensitive PI in response to a consumer’s “request to know” specific pieces of PI remains in place. However, the new draft regulations require a business to “inform the consumer with sufficient particularity” that it has collected this type of information. For example, a business should respond that it collects unique biometric data including a fingerprint scan without disclosing the actual fingerprint scan data. Businesses that do not collect PI directed from consumers: The new draft clarifies that businesses that do not collect PI directly from consumers and do not sell that information are not required to give notice to the consumer concurrent with the data’s collection. We view this additional provision as a helpful clarification. Previously, the regulations appeared to require consumer notice even in cases where a business had no direct relationship with the consumer. IP address as PI: The revised draft regulations delete a very helpful example from the February modifications of when IP addresses are not considered personal information. However, we believe that under the definition of personal information, IP addresses are only PI if they are reasonably capable of being linked to a particular person, given the information that the business already collects and maintains. The CCPA defines “personal information” as “information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household given information that the business already collects and maintains”. We expect additional guidance on when IP addresses qualify as PI to be put forth by California in the future, likely after the regulations are finalised or effective. Right to opt-out of sale if request to delete is denied: In the case where a business that sells PI denies a consumer’s 		



Development	Summary	Date	Links
	<p>request to delete their PI, the business’ response must offer the consumer the option to opt-out of the sale of the PI (provided that the consumer has not already requested to opt out). This provision was refined from the previous draft to require providing the opt-out link only in cases where the business denies the request to delete, instead of in all cases.</p> <p>7. Opt-out button deleted: The optional “opt-out button” graphic included in the February draft regulations has been deleted in the new draft. This graphic was to be used in addition to the required notice of the right to opt-out. This deletion has little practical effect as the graphic could not be used in lieu of opt-out notice and presumably it can still be used without any compliance impact.</p> <p>8. Service provider revised: Noteworthy is the rephrasing of what service providers are permitted to do with personal information. The new draft regulations state that a service provider may only process or maintain personal information “in compliance with the written contract for services required by the CCPA.” This unfortunate phrasing could be read broadly to imply that any contractual violation, regardless of its relation to the specific requirements of the CCPA, may be a regulatory violation as well—but we do not assess that California regulators (unlike European privacy regulators) will enforce any specific contractual clauses beyond the CCPA use limitation.</p> <p>9. Just-in-time notices: The revised regulations retain the provision added in February 2020 requiring a business that collects PI from a consumer’s mobile device for a purpose the consumer would not reasonably expect, to provide a “just-in-time” notice summarizing the categories of PI being collected and a link to the full notice of collection.</p> <p>Comments on the March 11, 2020 modified draft regulations may be submitted until 5 p.m. PST on March 27, 2020.</p>		



Development	Summary	Date	Links
California Privacy Rights Act anticipated to expand the California Consumer Privacy Act	<p>On November 4, 2019, a revised version of the proposed “California Privacy Rights Act” (“CPRA”) was submitted to the Office of the Attorney General. The CPRA would not be enforced until January 1, 2023 and only for violations occurring after that date.</p> <p>Among other things, the CPRA would:</p> <ul style="list-style-type: none"> – prohibit a business from retaining personal information for longer than reasonably necessary; – triple the maximum penalties for violations concerning consumers under age 16; – establish a California Privacy Protection Agency to enforce and implement consumer privacy laws, and impose administrative fines; – extend employee and business-to-business communications exemptions until January 1, 2023; and – expand the definition of “sale” to include the use of personal information to target individuals with ads that follow them as they browse the internet from one website to another. <p>If passed, the new legislation will require adoption of substantive regulations. The CPRA would require the issuance of regulations to clarify topics including: business purpose, requirements for cybersecurity audit, access and opt out rights for automated decision making and profiling and opt out by technical preferences. A summary of estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments estimates increased annual state costs of roughly \$10 million for a new state agency to monitor compliance and enforcement of consumer privacy laws.</p>	<p>Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021: 1 April 2020</p> <p>Anticipated Enforcement Date: 23 January 2023</p>	<p>Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021</p> <p>Link</p>



Spotlight on...

- **Ireland:** We discuss the new regulations allowing the Central Bank of Ireland to limit the GDPR rights of data subjects. [Read more...](#)
- **Ireland:** We examine the data protection implications on organisations during COVID-19. [Read more...](#)
- **UK:** We examine a recent High Court case that recognised of bitcoin as “property” following ransomware attack. [Read more...](#)
- **UK:** Cyber Security: What Managers Need to Know. [Read more...](#)
- **UK:** Commencement of the Protection of Personal Information Act – 1 April 2020. [Read more...](#)
- **US:** Accessibility – the Hidden A in the CCPA. [Read more...](#)
- **US:** Microsoft – Eversheds Sutherland whitepapers: responding to the evolving cyberthreat landscape in the financial services sector. [Read more...](#)
- **US:** Twisting in the wind—California attorney general issues revised CCPA Regulations. [Read more...](#)
- **US:** Biometrics litigation in healthcare—symptoms may include statutory damages. [Read more...](#)
- **Global:** We consider the data and cybersecurity issues arising from an increased reliance on alternative communication platforms during COVID-19. [Read more...](#)
- **US:** US cybersecurity and data privacy review and update: looking back on 2019 and planning ahead for 2020. [Read more...](#)

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



Rhoda Bryans

Associate

T: +44 20 7919 4769

rhodabryans@eversheds-sutherland.com



Thomas Elliot

Project Co-ordinator

T: +44 1223 44 3675

thomaselliott@eversheds-sutherland.com



Jananii Vanga

Trainee Solicitor

T: +44 734 207 3353

jananiivanga@eversheds-sutherland.com



Lauren Fishburne

Trainee Solicitor

T: +44 1223 44 3851

laurenfishburne@eversheds-sutherland.com



eversheds-sutherland.com

© Eversheds Sutherland 2020. All rights reserved.

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

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

Updated: edition 7