EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

October to December 2020

Executive summary

Welcome to the tenth edition of Updata!

Updata is an international report produced by Eversheds Sutherland's dedicated Privacy and Cybersecurity team – it provides you with a compilation of key privacy and cybersecurity regulatory and legal developments from the past quarter. This edition covers October to December 2020 and is full of newsworthy items from our team members around the globe. Of note, during that quarter we have seen updates including:

- COVID testing and remote working guidance across multiple jurisdictions;
- Increase in privacy enforcement action and litigation across many jurisdictions;
- the CJEU issued the judgment in the much anticipated *Privacy International* case concerning the mass use of surveillance technologies;
- not surprisingly, the Schrems II decision (which invalidated the EU-US Privacy Shield and requires additional due diligence before using the Standard Contractual Clauses) continues to feature prominently and the EDPB published recommendations for consultation in response;
- the European Commission published updated drafts of both the SCCs and controller-processor terms;
- California voters passed sweeping amendments to the California Consumer Privacy Act;
- The rampant SolarWinds hack, including the New York Department of Financial Services requirement to report on its effects;
- The Hong Kong Monetary Authority announced the launch of the enhanced Cybersecurity Fortification Initiative 2.0;
- China unveiled the full text of the draft Personal Data Protection Law of the People's Republic of China; and

We hope you enjoy this edition of Updata.

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

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

Click here to view contact information.

Follow us on Twitter at:
@ESPrivacyLaw

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
European Data Protection Supervisor issues guidance on DPIAs for large scale processing	The European Data Protection Supervisor ("**EDPS**") has stated that there are two factors to determine whether the processing of individuals' data was considered "large scale" processing under Article 39(3)(b) of Regulation (EU 2018/1725 on the processing of personal data by Union Institutions). These factors are: (1) the proportion of the relevant population; and (2) the nature of the personal data being processed and possible related risks. These factors are cumulative in suggesting a DPIA should be carried out.	1 October 2020	Newsletter
EPRS publishes its study on the Digital Services Act	The European Parliamentary Research Service ("**EPRS**") has published a study which analyses the potential value that could be added by enhancing the current EU regulatory framework on digital services. The study considers the current rules applicable to commercial entities operating online, and identifies gaps and risks for future improvement. It concludes by proposing policy solutions to tackle these issues.	1 October 2020	Study
CJEU issues *Privacy International* judgment	The CJEU has issued judgment in the case of *Privacy International*, and in the joined cases. The judgment states that member states cannot carry out unlimited mass surveillance of phone and internet data. However, where a member state is facing a serious threat to national security, the member state may order electronic communications services providers to retain traffic data and location data. The period of such general and indiscriminate retention must be limited to what is strictly necessary. Individuals suspected of involvement in terror activities can be subject to real-time surveillance of traffic data and phone data.	6 October 2020	Press release Judgment Joined cases judgment

General EU and International

Development	Summary	Date	Links
EU Commission launches 2021 work programme	The Commission has launched its 2021 work programme, which includes making Europe 'fit for the digital age', through a focus on the right to privacy and connectivity, freedom of speech, free flow of data and cybersecurity. The programme includes a legislative agenda which will cover AI and the European e-ID.	19 October 2020	Press release Work programme
EU interoperability gateway for COVID-19 tracing apps goes lives	An EU-wide gateway for contact tracing apps has been launched following a successful pilot phase. The national apps from Germany, Ireland and Italy are the first to be linked through the service. The gateway is designed to allow national tracing apps to interact with apps from other Member States and work across borders to halting the transmission of Covid-19. The gateway can work with 20 apps – it is expected that the next update will link the apps from the Czech Republic, Denmark, Latvia and Spain. The gateway means users will only need to install one app, which will then work across participating Member States. Data exchange is kept to a minimum – only arbitrary identifiers will be transferred between national apps. Information is pseudonymised, encrypted, and kept only as long as necessary to track infections. Individuals cannot be identified, nor can their location or movement be tracked. The gateway will be operated from the Commission's data centre in Luxembourg.	19 October 2020	Press release
Next generation cloud for Europe welcomed by the European Commission	The European Commission and German Presidency of the Council of the EU have issued a statement welcoming the joint declaration published by 25 Member States on the next generation cloud for the EU. The Commission has highlighted the importance of the joint approach in supporting European businesses and providing European citizens choice in data processing infrastructure and services. Under the joint declaration, the Member States agree to work together to creating resilient and competitive cloud infrastructure and services across the EU. The aim is to benefit European businesses and the public sector, providing safe data storage and maintenance. Member States have also agreed to combine investment from private, national and EU bodies to create a common technical and policy approach to the cloud. In the beginning of 2021, a European Alliance on Industrial Data and Cloud is expected to be launched.	15 October 2020	Press release Article Joint declaration

General EU and International

Development	Summary	Date	Links
Guidelines on Data Protection by Design and Default adopted by EDPB	The European Data Protection Board ("**EDPB**") adopted Guidelines on Data Protection by Design and Default during its 40th plenary session. The Guidelines are focused on the obligation in Article 25 GDPR – that is, the effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default. A coordinated enforcement framework was established by the EDPB, to coordinate recurring annual activities by EDPB Supervisory Authorities. Such activities will include joint awareness raising, information gathering, enforcement sweeps and investigations. The EDPB also adopted a letter outlining the data protection implementation of Article 17 of the Copyright Directive, in relation to upload filters. The letter stated that any processing of personal data for upload filters must be proportionate and necessary, and as far as possible, no personal data should be processed when Article 17 is implemented.	21 October 2020	Press release Agenda
EDPB adopts recommendations following *Schrems II and publishes for consultation*	Following the *Schrems II* court decision this summer, which both invalidated the Privacy Shield framework for transfers of personal data from the EU to the US and, simultaneously, cast doubt on whether standard contractual clauses ("**SCCs**") provide adequate protection for data transfers, the EDPB has adopted recommendations on measures to ensure compliance with EU data protection requirements when transferring personal data outside of the European Economic Area ("**EEA**"). These recommendations were open for consultation until 21 December 2020 (extended from 30 November 2020). These recommendations have been eagerly anticipated by privacy professionals. Briefly, by way of background, GDPR requires that personal data can only be transferred outside of the EEA if it is adequately protected. Unless a derogation under GDPR applies, in practice this means that either: (i) the territory to which the personal data is transferred has received an 'adequacy decision' from the EU (rare); (ii) the appropriate version of SCCs is put in place between the data exporter and importer; or (iii) the transfer is pursuant to binding corporate rules (only available for companies within the same corporate group, and is rarely relied upon in practice). SCCs	11 November 2020	Press release Recommendations – measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Recommendations – European Essential Guarantees for surveillance measures ICO statement

Development	Summary	Date	Links
	are by far the most commonly relied upon mechanism for exporting personal data to outside the EEA. Following the *Schrems II* court decision, a controller using SCCs to export personal data must take steps to ensure that the data importer entering into the SCCs can actually comply with the terms of the SCCs – i.e. the controller must take steps to verify if the legal regime of the third country (to which the data importer is subject) would prevent the SCCs from being complied with, which would prevent the personal data being protected by 'essential equivalence'. Data exporters may use measures in addition to SCCs to comply with their duty to ensure equivalence with European data protection standards, where SCCs are not sufficient. The EDPB's recommendations aim to assist data exporters in identifying and using appropriate supplementary measures where necessary. A roadmap is included to help data exporters assess whether data transfers are in accordance with EU law, and which measures may be appropriate to ensure this. However, the EDPB has highlighted that responsibility lies with data exporters in making the crucial assessment of equivalence (and necessary supplementary measures); due diligence must be thorough and must be properly recorded in line with accountability under the GDPR. The EDPB has also stressed that supplementary measures may not be sufficient in all cases. The key recommendations are as follows: – data exporters must know their transfers, i.e. be aware of where personal data is being transferred to; and ensure that transferred data is 'adequate, relevant and limited' to what is necessary for the purpose and processing; – verification of transfer mechanisms used to export the personal data (i.e. an adequacy decision, SCCs, binding corporate rules or a derogation); – assess if the third country's laws or practices may limit the effectiveness of the safeguards of the transfer tools used. Importantly, this is significantly broader than simply assessing whether the surveillance laws in the third country may compel the data importer to process personal data outside of what is permitted under SCCs, binding corporate		

Development	Summary	Date	Links
	rules etc (although see further detail below about surveillance assessment); – identify and adopt necessary supplementary measures to ensure essentially equivalent data protection (e.g. technical measures, additional contractual measures, organisational measures); – take formal procedural steps if required (as summarised in the recommendations); and – re-evaluate throughout the protection given to transferred data and monitor if any developments affect the protection of transferred personal data. In relation to assessing equivalence for surveillance laws, EDPB has published separate recommendations which contain useful detail as to how data exporters can assess whether the third country's laws/regime provides for the same level of 'essential guarantees', which means (according to the recommendations): – processing should be based on clear, precise and accessible rules; – necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; – an independent oversight mechanism should exist; and – effective remedies need to be available to the individual. In the UK, the Information Commissioner's Office ("**ICO**") has published a statement that it is reviewing the recommendations.		
European Commission publishes draft (updated) SCCs (and launches public consultation)	The European Commission has published a draft set of updated SCCs ("**New SCCs**"), which were open for consultation until 10 December 2020. This update has been eagerly anticipated by privacy professionals, and is intended to replace the existing forms of SCCs in due course (which had not yet been updated following GDPR). Notably, the New SCCs are a single document which covers obligations relating to controller-controller transfers, controller-processor transfers, processor-processor transfers and processor-controller transfers. Currently, the former two categories are dealt	12 November 2020	Draft implementing decision and annex

Development	Summary	Date	Links
	with in different versions of SCCs (and, indeed, controller-controller transfers have a choice of two different forms of SCCs), whilst the latter two categories do not currently have specified SCCs and the New SCCs will therefore plug an existing gap (in particular the introduction of obligations in relation to processor-controller transfers). Amongst other obligations in the SCCs are obligations of the data importer in relation to any government authority's access requests to personal data transferred pursuant to the New SCCs – a hot topic following the *Schrems II* decision.		
European Commission publishes draft controller-processor terms	In addition to published draft New SCCs (see update above), the EU Commission has also published an updated draft of standard terms to be entered into between controller and processor as set out in Article 28 GDPR. Briefly, by way of background, when a controller engages a processor, Article 28 GDPR sets out some (minimum) obligations which must be contained in a written agreement between the controller and processor. GDPR empowered the EU Commission to lay down standard contractual terms to cover the Article 28 GDPR requirements, and now the EU Commission has published a draft of such terms for public consultation (the consultation closed on 10 December 2020) ("**Draft Processor Clauses**"). Interestingly, the Draft Processor Clauses go beyond the (minimum) requirements of Article 28 GDPR – for example, providing that not only must a processor notify the controller of personal data breaches '*without undue delay*' (which is what GDPR requires), but that in addition it will do so in any event within 48 hours (this timescale is not set out in Article 28 GDPR itself). Furthermore, in relation to audit rights, it makes clear that should a processor mandate an independent auditor (e.g. for the purposes of sharing an audit report with the controller), the processor must bear all of the costs of the audit – which party is responsible for the cost of audits is also not addressed in the GDPR. However, in other regards, the Draft Processor Clauses do not go further than Article 28 GDPR requirements (e.g. where the parties agree that the processor is authorised to engage sub-processors without prior consent, but subject to a requirement to notify the controller in	12 November 2020	Draft implementing decision and annex

Development	Summary	Date	Links
	advance of changes to sub-processors thereby giving the controller the chance to object, which is the minimum GDPR requirement, the Draft Processor Clauses are silent (like the GDPR) on what happens if the controller does object). Usefully, the Draft Processor Clauses contain (in square brackets) some information security areas which could be covered in the Annex III and are intended to work as a description of the technical and organisational security measures which the processor must implement to protect personal data (the same concept is addressed in the New SCCs mentioned in the update above).		
Revised draft of the ePrivacy Regulation published	The Presidency of the Council of the European Union has published a revised text for the proposed ePrivacy Regulation (Regulation concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)). The latest draft has followed much debate and is likely to garner even more deliberation. It includes, amongst others, the removal of some provisions around retention of information and increased clarity around necessity in the context of use of terminal equipment to provide services to users.	4 November 2020	Draft Regulation
WHO and UN (and others) joint statement on data protection and privacy (in relation to COVID-19)	The United Nations, World Health Organisation and a number of other international bodies have issued a joint statement promoting the respect for privacy rights in relation to the COVID-19 response. The high-level statement recognises the important role that collection and use of data can play in responding to the pandemic, including via digital contact tracing, analysis of mobility data etc. However, it is acknowledged that this could have a significant impact if used for purposes not specifically related to the COVID-19 response, and on that basis the statement contains a summary of the principles which UN system organisations must comply with in this context (including security, retention and transparency amongst other principles).	19 November 2020	Joint statement

Austria

Contributors

Georg Roehsner
Managing 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
Regional High Court of Vienna largely confirms judgment against Max Schrems in his suit to be considered a controller over personal data on a social media site	Austrian privacy activist Max Schrems had filed a lawsuit against a global social media company at the Regional Court of Vienna. Amongst other claims, Schrems requested the court to – order the company to provide Schrems with complete data access under Article 15 GDPR; – rule that Schrems himself is controller of the processing of his own personal data in his social media profile, while the company is only the processor; – require the company to conclude a Data Processor Agreement under Article 28 GDPR with Schrems and to order it to cease all processing which Schrems has not instructed pursuant to Article 28 (3a) GDPR; – rule that accepting the company's Terms of Service does not constitute valid consent under GDPR; – require the company to cease processing Schrems' personal data for personalised advertisement: in connection with Social Plugins; in the context of the application "Graph Search"; or in the context of personal data collected from third parties without Schrems' consent.	28 December 2020	Link to statement by Max Schrems/noyb (in English) Link to the decision (in German) Link to English Machine Translation of the decision (created by noyb)

Development	Summary	Date	Links
	The Regional Court of Vienna ruled on this case on 30 June 2020 (see our Updata entry on Q3/2020). It ordered the company to provide Schrems with complete data access under Article 15 GDPR and awarded €500 in damages to Schrems for this violation.The other claims were denied, some on formal grounds, others as the court did not consider the company to be in violation of GDPR. Both parties appealed against this decision to the Regional High Court of Vienna. The Regional High Court of Vienna has now decided on these appeals and both appeals were denied (and the original decision by the Regional Court of Vienna was upheld). Schrems has announced that he will appeal against this decision to the Austrian Supreme Court. He will also request that the Supreme Court file a request for preliminary ruling to the ECJ.		
Federal Administrative Court: Google may provide access under Article 15 GDPR via its online tools, there is no general right to a hardcopy response	The claimant sent a data access request to Google. Google replied by asking the claimant to access the data processed in the context of his Google account and additional information on the processing via his Google account. For data that was not accessible via the claimant's Google account, Google requested that the claimant to use an online form accessible via the Google account, to ensure that the claimant would only receive personal data related to him (and not some other data subject). The claimant refused and filed a complaint at the Austrian DPA. Following an appeal against the DPA's decision, the Federal Administrative Court denied most parts of the claim regarding the right to access. It ruled that Google is allowed to request data subjects that want to access their personal data under Article 15 GDPR to log into their Google account to access their data there. Google is also allowed to use an online form in order to identify and authenticate the requesting data subject for all data that is processed outside of the Google account.	Date of decision: 28 December 2020 Published: 1 October 2020	Link to the decision (in German)
Federal Administrative Court overturns €18m penalty against Austrian Postal Service	The Austrian Postal Service had been selling data on Austrian residents' "affinity for a political party", which it had calculated/assumed from other data collected about these individuals.	Date of first decision: 20 August 2020	Link to the first decision (regarding the violation of GDPR; in German)

Development	Summary	Date	Links
	In January 2019, the Austrian DPA ruled against the Austrian Postal Service. It held that data about the assumed "affinity for a political party" of an individual is considered special category data under Article 9 GDPR. The Austrian Postal Service would therefore have required the data subjects' consent for processing this data. A penalty of €18m was issued against the Austrian Postal Service for this violation. The Austrian Postal Service appealed to the Federal Administrative Court. In three decisions (one dated 20 August 2020 and two dated 26 November 2020), the Federal Administrative Court partially upheld the DPA's assessment of the case and confirmed that data about the assumed "affinity for a political party" is indeed considered special categories of data under Article 9 GDPR and that the Austrian Postal Service's data processing therefore violated GDPR. However, the Court overturned the penalty of €18m and held that penalties under Article 83 GDPR must be issued in accordance with the principles of the national law of administrative procedure. According to §§ 44a and 45 of the Austrian Act on Administrative Penalties (Verwaltungsstrafgesetz – VStG) and § 30 of the Austrian Data Protection Act (Datenschutzgesetz – DSG), a penalty under GDPR may only be issued against a legal person, if the DPA can prove culpable conduct of natural persons acting on behalf of this legal person. As the DPA had failed to establish such culpable conduct, the penalty violated procedural law and was overturned. It should be noted that this fine was overturned only due to a formal error by the DPA. The data processing itself was deemed unlawful. It is to be expected that both parties will appeal to the Austrian Administrative Supreme Court.	Date of second and third decision: 26 November 2020	Link to the second decision (regarding the violation of GDPR; in German) Link to the third decision (regarding the penalty; in German)
Austrian DPA: New guidelines regarding processing of personal data in the context of Covid-19	On 1 October 2020, the Austrian DPA updated its guidelines regarding processing of personal data in the context of Covid-19. In this update, the DPA again clarified that it may be permissible under Article 9 (2b) GDPR to require employees to take a Covid-19-PCR test, if this is required to prevent the spread of the infection within a company.	1 October 2020	Link to the guideline (in German)

Development	Summary	Date	Links
	The Austrian DPA criticised the newly instituted requirement for restaurants to register their guests and retain their data for contact tracing purposes in certain regions of Austria, stating that such measures require a legal basis fulfilling the requirements under Article 9 (2i) GDPR. The DPA voiced doubts as to whether the current legal provisions in Austria meet these requirements. Following this criticism, a new legal basis for such measures was introduced in December 2020 (§ 5c Austrian Epidemy Act – Epidemiegesetz).		
Federal Administrative Court: Information stored by a religious community in a sealed envelope is not subject to the right to access	The claimant filed a request under Article 15 GDPR requesting a copy of all documents related to his exclusion from a religious community. These documents were stored in a sealed envelope. As this request was denied, the claimant filed a complaint at the Austrian DPA. Following an appeal to the Federal Administrative Court, the Court rejected the claim. It ruled that the documents stored in a sealed envelope are not to be considered part of a filing system pursuant to Article 2 GDPR. Therefore, the GDPR is not applicable and the right to access does not apply. Furthermore, the right to access does not grant the right to receive copies of administrative documents. As the religious community in question has been granted the status of a legal person under public law, the documents in question are to be considered administrative documents. Therefore, the right to access – even if it were applicable – does not grant a right to receive a copy of these documents.	Date of decision: 1 October 2020 Published: 21 October 2020	Link to the decision (in German)
Austrian DPA: €600 penalty against doctor for publishing patient data on social media	A medical doctor published information about their patients, including health data, names and social security numbers and excerpts from medical records on its personal social media page. The Austrian DPA held that this was a violation of Articles 5(1a) and 9 GDPR. The DPA issued a penalty of €600 for this violation.	Date of decision: 1 October 2020 Published: 27 November 2020	Link to the decision (in German)
Austrian DPA: Postal Services may make a copy of ID documents of recipients of registered mail	The claimant in this case had been informed by the Postal Service that a registered letter addressed to him could be picked up at his local Postal Office. When the claimant came to pick up the letter, the employee at the counter requested ID and made a copy of the claimant's ID document. From this copy, the Postal Service automatically	Date of decision: 1 October 2020 Published: 2 December 2020	Link to the decision (in German)

Development	Summary	Date	Links
	extracted the following data: type of ID card, ID card number, issuing authority, date of birth, name. This information was retained for 6 months and then deleted. The copy itself was not retained. The claimant filed a complaint against this practice at the Austrian DPA. The complaint was denied. The Austrian DPA ruled that the Austrian Postal Service has a legitimate interest in collecting and retaining kind form of data in order to protect itself against potential legal claims by the sender of the letter. The DPA ruled that the Austrian Postal Service had adhered to the principles of data minimisation and storage limitation. The complaint was therefore denied.		
Austrian DPA: Quarterly Report	Quarterly Report by the Austrian DPA – in this report, the DPA focusses on GDPR requirements in the context of customer loyalty programmes.	23 October 2020	Link to the newsletter (in German)

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
Draft Personal Data Protection Law《个人信息保护法（草案）》	On 21 October 2020, China unveiled the full text of the draft Personal Data Protection Law of the People's Republic of China ("**Draft PDPL**"). The Draft PDPL comprises a total of 8 chapters and 70 articles covering a variety of data protection principles, including transparency, fairness, purpose limitation, data minimisation, limited retention, data accuracy and accountability. Generally speaking, the Draft PDPL echoes most of the requirements for protection of personal data in the existing laws and makes such requirements legally enforceable. In addition, the Draft also raises some new concepts. These include, amongst others: – Effect of extra-territorial application - the Draft PDPL provides for extra-territorial application to certain personal data processing activities outside the PRC. It also requires certain foreign personal data processors to set up specialised agencies or appoint designated representatives in the PRC to deal with data protection related matters. Further, the Draft PDPL grants the regulatory authorities the power to put organizations or individuals on a "blacklist" which would in	21 October 2020	Draft Personal Data Protection Law

Development	Summary	Date	Links
	turn restrict their ability to or prohibit them from receiving personal data from China. – "Specific consent" required from data subjects - the Draft PDPL raised a new concept of "specific consent" which is required to be obtained by data processors from data subjects prior to certain types of personal data processing. – Processing of personal data that has already been disclosed to public – the existing law does not require consent to be obtained for collection and use of personal data that has been proactively disclosed by data subjects to the public. The Draft PDPL, however, imposes certain restrictions on the processing of this category of personal data. – Data localisation and cross border data transfers - the Draft PDPL proposes a new regulatory mechanism for the localisation and cross border transfers of personal data. This new mechanism is materially different from the existing one, and specifically set out the data localisation requirements and regulatory control measures required prior to exporting personal data for each of the six categories of targeted data processors/ types of data export. The requirements range from the more stringent side of the spectrum, aimed at government departments and Critical Information Infrastructure operators, to the more lenient side, aimed at data export in accordance with international treaties. – Administrative penalties – the Draft PDPL imposes harsher penalties for violations than the Cybersecurity Law. Serious violations may lead to a fine of up to RMB 50,000,000 or 5% of the offender's preceding year's revenue. It also imposes personal liability, the personnel who is directly responsible for the personal data processing activities may be fined up to RMB 1 million.		
Information Security Technology – Guidance for Personal Data Security Impact Assessment《信息安全技术 个人信息安全影响评估指南》	On 19 November 2020, the State Administration for Market Regulation and the Standardization Administration of China jointly promulgated the Information Security Technology – Guidance for Personal Data Security Impact Assessment (the "**Guidance**"). The Guidance sets out basic principles and implementation procedures for personal data security impact assessments	Published: 19 November 2020 Effective: 1 June 2021	Information Security Technology – Guidance for Personal Data Security Impact Assessment

Development	Summary	Date	Links
	(applicable to all organizations). The principles and procedures set out therein also provide reference to the regulatory authorities, third-party assessment institutions and other similar organizations conducting supervision, inspection and assessment works in relation to personal data security. The Guidance further provides, in its appendices, examples illustrating how such assessment should be conducted in different scenarios and the personal data processing activities that present high risks to the subject of the relevant personal data, as well as a template assessment form and assessment criteria prepared in accordance with the Guidance itself.		
Network Security Standard Practice Guide—Security Guidelines for the Use of Software Development Kit (SDK) for Mobile Internet Applications (App) **《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》**	On 27 November 2020, the Secretariat of the National Information Security Standardization Technical Committee published the Network Security Standard Practice Guide—Security Guidelines for the Use of Software Development Kit (SDK) for Mobile Internet Applications (App) (the "**Practice Guide**") to give guidelines on the security practices for the use of SDK in Apps. Apart from introducing the relevant parties and obligations in the use of SDK in Apps and the common types of SDK, the Practice Guide further elaborated on the common security issues in the use of SDK in Apps, which include loopholes in the SDK itself, malicious behaviours of the SDK, and illegal collection and use of personal data by the SDK. It also sets out basic security principles that are to be followed in the use of SDK by Apps, as well as suggested safety measures to be adopted by App and SDK providers respectively.	27 November 2020	Network Security Standard Practice Guide—Security Guidelines for the Use of Software Development Kit (SDK) for Mobile Internet Applications (App)
Draft Scope Of Necessary Personal Data to be Collected by Mobile Internet Applications (App) **《常见类型移动互联网应用程序（App）必要个人信息范围（征求意见稿）》**	On 1 December 2020 the Cyberspace Administration of China published the Draft Scope Of Necessary Personal Data to be Collected by Mobile Internet Applications (App) (the "**Draft Scope**") for public consultation. The Draft Scope aims to implement the principles of legal, proper and necessary collection of personal data specified in the Cybersecurity Law, standardise personal data collection behaviours of Apps and ensure security of the public's personal data. The Draft Scope specified the scope of "necessary personal data" for 38 Apps in common use. This term refers to personal data	1 December 2020	Draft Scope Of Necessary Personal Data to be Collected by Mobile Internet Applications (App)

Development	Summary	Date	Links
	necessary to ensure the normal operation of the basic functions of the relevant App, without which the App cannot provide its basic functional services. As long as the user agrees to the collection of these "necessary personal data", the App must not refuse the user's installation and use. The types of Apps that were regulated by the Draft Scope includes apps for map navigation, online car-hailing, instant messaging, online-shopping apps and renting and selling of real property.		

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

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

Development	Summary	Date	Links
The CNIL issued updated guidelines and recommendations regarding cookies and other tracers	On 4 July 2019, the CNIL adopted new guidelines on cookies and tracers, to align the rules applicable to such technologies with the principles of the GDPR. On 19 June 2020, the Conseil d'État (French administrative supreme court) approved most of the guidelines, but struck down the section in which the CNIL indicated that access to a website could never be made conditional on the acceptance of cookies. The CNIL's updated guidelines of 17 September 2020 (published on 1 October 2020) were therefore modified to remove any general prohibition of cookie walls. In addition, on 14 January 2020, the CNIL published its draft recommendation on cookies and tracers and launched a public consultation. The final version of the recommendation adopted on 17 September 2020 includes the contributions the CNIL received during the public consultation. The CNIL intends for these recommendations to serve as a practical guide for website	Date of CNIL's recommendations: 23 October 2020 Date of CNIL's statement: 1 October 2020	CNIL's recommendations (in French) CNIL's guidelines (in French) CNIL statement (in French) CNIL's FAQ (in French)

Development	Summary	Date	Links

	operators setting out how consent for cookies and tracers can be obtained.
	
	The CNIL's updated guidelines and final recommendations include a number of general principles on how to validly install cookies and tracers on a user's device:
	
	– As regards the consent of users:
	  – Continuing to browse or use a website can no longer be considered as valid consent for the installation of cookies and other tracers;
	  – Users must consent to the installation of cookies and tracers by a clear positive act (e.g. clicking an "accept" button);
	  – Users must be able to withdraw their consent easily and at any time; and
	  – Refusing tracers should be as easy as accepting them.
	– As regards the information to be provided to users:
	  – Users must be clearly informed about the purposes of the cookies and tracers before accepting them, and about the consequences of accepting or rejecting cookies and tracers; and
	  – They must also be informed about the identity of all parties using the cookies for which consent is collected.
	– Organisations using cookies and tracers must be able to provide, at any moment, proof that free, informed and specific consent has been obtained from each user.
	– Some cookies and tracers listed by the CNIL are exempt from the requirement of collecting consent.
	
	The CNIL set out detailed guidance and practical advice about each of these requirements in the guidance and recommendations. It has also published a FAQ on its website.
	
	A period of grace of 6 months (from the date of the publication of the guidelines and recommendations) applies to enable website operators to implement the necessary modifications. The CNIL will		

Development	Summary	Date	Links
	start conducting checks to verify compliance with the new rules after this grace period.		
Facial recognition in airports: challenges and main principles to be complied with	Since biometric facial recognition devices are increasingly used in airports, the CNIL has been asked by airport managing bodies and service providers to assist them in the experimentation of such technologies, and it has therefore clarified its position in this regard. In its statement, the CNIL highlights that facial recognition involves the processing of biometric data, and that biometric data qualifies as sensitive data under the GDPR and should therefore be handled carefully. Several principles must therefore be complied with when conducting biometric controls within airports, including: – Justifying the necessity and proportionality of the facial recognition system; – Collecting the prior, free, specific and informed consent of the passengers; – Complying with the privacy by design and by default principles, as well as the principle of data minimisation, including by storing biometric data either on a medium over which the passenger has exclusive control and use, or in a database under an encrypted form; and – Conducting an Data Protection Impact Assessment before launching the processing activity. The CNIL's recommendations provide detailed guidance about how to comply with these general principles.	9 October 2020	CNIL statement (in French)
The CNIL publishes recommendations about the collection of personal data by restaurants for Covid-19 contact tracing	The French authorities required public establishments such as restaurants to list the names and contact details of all customers, in order to allow health authorities to obtain the necessary information for contact tracing in case a client of a restaurant is tested positive to Covid-19. The CNIL therefore clarified the rules to be complied with by restaurants in relation to this personal data processing, which includes inter alia the limitation of the collection to necessary data,	7 October 2020	CNIL statement (in French)

Development	Summary	Date	Links
	the disclosure of the list only to public health authorities, the provision of appropriate information to data subjects, the limitation of the retention period and the implementation of adequate security measures. The CNIL also provided templates of forms which could be used by restaurants to collect the contact details of customers, and which notably include the required privacy information.		
The CNIL issues a reference document for the social and medical social professions	The CNIL's draft reference document is directed to private or public organisations who accommodate or provide social and/or medico-social support to the elderly, people with disabilities or people in difficulty. It provides guidance on how these entities may provide services to the data subject, process personal data in relation to the payment of social benefits, provide social and medico-social support adapted to the difficulties encountered by the data subject, develop personalised support projects, etc. This reference document will not be binding. Data controllers may depart from the CNIL's recommendations (for example, by identifying other legal bases for a specific processing activity, etc.), provided they can justify their choice. A separate reference document will be published about the childcare sector in view of the specific nature of such processing activities. The draft reference document about the social and medico-social sectors was subject to public consultation until 1 December 2020.	12 October 2020	CNIL statement (in French)
The CNIL publishes guidelines about health data and sporting establishments	Many organisations have contacted the CNIL as they wish to implement measures to limit the spread of Covid-19 and protect the health of participants to sporting activities and events (including athletes, coaches and referees). The CNIL has emphasised that any temperature taking, any result of a RT-PCR test, and any medical certificate provided to assess a risk of exposure to Covid-19, constitute health data within the meaning of the GDPR. The CNIL further clarifies that the processing of health data is, in principle, prohibited and that health data may, by exception, be	14 October 2020	CNIL statement (in French)

Development	Summary	Date	Links
	processed by sports organisations if they are in one of the following situations: – The sports structure obtains, prior to the collection of health data, the consent of the data subjects (athletes, coaches, referees, etc.). Consent will nevertheless not be considered valid if it is not freely given (e.g. if refusal to provide the results of a RT-PCR test or to undertake a temperature testing prevents access to the sporting practice or to a facility). – The collection of health data is justified by important public interest. Sporting establishments may rely on this ground when a specific legislation or regulation authorises the collection of health data in relation to a sports activity in the context of COVID-19. The CNIL also provides specific guidance on the measures that can be taken by organisations in relation to the prevention of Covid-19.		
Practical recommendations regarding the processing of personal data after the death of a data subject	As a reminder, the French Data Protection Act offers data subjects the right to define instructions about the management of their personal data after their death. However, in the absence of a request from the heirs or relatives, the profiles of deceased persons are often not deleted, in particular on social media. In practice, it is difficult for website operators to distinguish between inactive users and deceased users, and they do not take the initiative to delete accounts if they do not know the reason for the absence of activity on the account. The CNIL has therefore clarified the rules applicable to the online accounts of a deceased person, which notably include the following: – Heirs or relatives cannot access the online accounts of a deceased person, since social media profiles and email accounts are subject to the secrecy of correspondence. – Heirs or relatives can update the profile of a deceased person to inform third parties of his/her death.	28 October 2020	CNIL statement (in French)

Development	Summary	Date	Links
	– It is also possible to have the account of a deceased relative deleted, in the absence of a directive to the contrary from this person. – Heirs may bring an action before the courts if the reputation of a deceased relative is damaged or they suffer another prejudice. Additional guidance is provided in the CNIL's statement about how to contact social media or messaging services operators.		
French highest administrative court approved the governmental facial recognition app	By a decree dated 13 May 2019, the French government authorised the creation a facial recognition application named "Alicem". This mobile app aims at enabling its users to "authenticate" themselves electronically (in accordance with the eIDAS regulation). In practice, the user has to register his or her biometric passport or residence card, the chip's information are obtained through NFC and the individual's face is compared with the photograph of his or her passport or residence card. The user can thus use this application to confirm his or her identity with public entities or partner private entities. The creation of "Alicem" has raised concerns, especially regarding the possible tracking of individuals by the State or private companies. A French association who defends the rights and freedoms of Internet users therefore brought an action before the French highest administrative court, the Conseil d'Etat, to request the annulment of the decree which authorised the creation of this facial recognition app. However, the Conseil d'Etat rejected the annulment request. It reminded the participants that the processing of biometric data is prohibited unless (i) the data subject provides his or her explicit consent, and (ii) for processing based on important public interests, the processing activity is proportionate. According to the Conseil d'Etat, there are no other means of authenticating the user's identity electronically as reliable as facial recognition systems. The processing of biometric data is therefore justified with regard to the purpose of the processing. In addition, users are not obliged to register on the "Alicem" app.	4 November 2020	Decision (in French)

Development	Summary	Date	Links
	They can always use other online identification technologies which do not involve the use of facial recognition.		
The CNIL's FAQ on remote working	The CNIL has answered the practical questions it frequently receives regarding remote working, notably during the Covid-19 pandemic. In its FAQ, the CNIL reminds the public that derogatory rules have been implemented in labour law regarding teleworking during the epidemic, and provides answers about a number of practical matters, including: – the conditions under which an employer can control the activity of employees who are working remotely; – whether an employer can constantly monitor the employees, including examples of systematic surveillance methods which are prohibited; – the precautions to be taken when employees use their personal mobile phones, computers or tablets; – whether an employer can compel the employees to turn on their cameras during video calls, etc.	12 November 2020	CNIL statement (in French)
The CNIL publishes a draft reference document about rental management	The CNIL's reference document is directed to professional lessors. The CNIL however clarifies that it can also be used by non-professional lessors, as well as by tenants (as data subjects, in order to understand how their personal data can be collected and processed). The CNIL covers all the stages of a property lease: the offer of properties for rent, the conclusion of the lease contract, the management of the lease (lease payments, etc.) and the termination of the lease. This reference document will not be prescriptive, it aims at guiding professionals in bringing their activities in compliance with data protection laws and in conducting a Data Protection Impact Assessment where necessary. However, professionals who will depart from the CNIL's guidelines must be able to justify their choice.	17 November 2020	CNIL statement (in French)

Development	Summary	Date	Links
	The draft was subject to public consultation until 18 December 2020. A consolidated version was then be presented to the CNIL's members for final adoption.		
The CNIL issues a draft recommendation on the exercise of data protection rights through a proxy	The CNIL's draft recommendation defines the conditions under which a data subject may designate a company to exercise, on his or her behalf, the rights granted to him or her by the GDPR and the French data protection act. This recommendation is directed to companies acting as proxies of data subjects, but also to data controllers who receive right requests from companies appointed as representatives by the relevant data subjects.The recommendation will not be prescriptive, but could be used as a practical guide by the representative companies and the controllers. The draft recommendation notably covers the following points: – the form and content of the power of attorney to be received by the representative company; – automated requests for the exercise of data protection rights; – the situations in which a controller may consider a request by a representative as complex, manifestly unfounded or excessive; – the security standards to be implemented and the formats to be used for the transmission of personal data; and – the conditions under which an authorised representative may re-use for its own account the personal data it has collected on behalf of a data subject. The CNIL also provides a template power of attorney to which companies acting as representatives of data subjects or data controllers can refer. The CNIL's draft recommendation is subject to public consultation until 6 January 2021. After this period, a new version of the recommendation will be presented to the CNIL's members for final adoption.	25 November 2020	CNIL statement (in French)

Development	Summary	Date	Links
The CNIL imposes a € 3.25m penalty on French retail group for breaches regarding transparency and compliance with right requests	The CNIL imposed a fine of €2.25 million on Carrefour France and a fine of €800,000 on Carrefour Banque for various violations on the GDPR and the French data protection act. The CNIL had received several complaints against these two affiliates of the French retail group Carrefour, and therefore carried out investigations at these two companies between May and July 2019. The CNIL noted several breaches of applicable data protection laws, including: – Breaches of the obligation to provide appropriate information to data subjects. The information provided to users of the Carrefour France' and Carrefour Banque's websites, and to clients wishing to join the loyalty program or the payment card program was not easily accessible nor understandable. Indeed, information about personal data processing was fragmented among several documents, which were lengthy and contained large amounts of other information, and was provided in broad and vague terms. – In addition, the information provided to data subjects was incomplete. In particular, the CNIL found that the information provided about data retention was insufficient. The information provided on the websites did not specify the retention periods. Only general terms such as "personal data are retained for the applicable statute of limitation periods" were provided. Information was also insufficient regarding data transfers outside the European Union and the legal basis for the processing activities. – Breaches regarding consent for non-essential cookies Cookies that were automatically installed on the terminals of users who accessed the Carrefour France's and Carrefour Banque's websites, prior to any action from such users. The cookies included non-essential cookies used for advertising purposes, including Google Analytics cookies, and should therefore not have been installed on the users' terminal without their consent. – Breaches of the obligation to limit personal data retention The CNIL found that Carrefour France defined an excessive	Date of CNIL's decisions against Carrefour France and Carrefour Banque: 25 November 2020 Date of CNIL's statement: 26 November 2020	CNIL's decision against Carrefour France (in French) CNIL's decision against Carrefour Banque (in French) CNIL statement (in English)

Development	Summary	Date	Links
	retention period (4 years) for the members of its loyalty program. In addition, personal data was kept beyond this retention period, since it was identified that Carrefour France retained, in relation to the loyalty program, the personal data of more than 28 million customers who had been inactive for 5 to 10 years. Similarly, Carrefour France had retained the personal data of 750,000 users of the carrefour.fr website who had been inactive for 5 to 10 years. – Breaches regarding data subjects' right requests The CNIL identified that Carrefour France failed to facilitate the exercise by data subjects of their data protection rights, since it required a proof of identity for any right request, which was not justified when there was no doubt about the identity of the data subject. – In addition, this entity failed to respond to a number data subjects' requests within the deadlines set forth by the GDPR, or to comply with several requests (including in relation to deletion of personal data or objection to advertising communications). – Breaches of the obligation to process personal data fairly. When members of the payment card program wanted to join the loyalty program, they had to tick a box to indicate that they agreed that Carrefour Banque would share their name and email address to another entity of the group. It was expressly indicated that no other personal data would be disclosed, while in fact other types of personal data were shared with Carrefour France, including postal addresses, phone numbers and number of children. Despite the fact that all identified breaches had been remedied as per the CNIL's instructions, the CNIL decided to impose a financial penalty on both companies because of the seriousness of the breaches identified and the period of time during which they were committed.		
Decision of the French Supreme Court, concerning the use of personal data for evidentiary	In this case judged on 25 November 2020 by the French Supreme Court (Cour de Cassation), an employee, who was also the DPO, had been dismissed for serious misconduct for having sent five electronic requests for information to a competitor company by	25 November 2020	Decision of the Cour de cassation (in French)

Development	Summary	Date	Links
purposes in the context of a labour law litigation	appropriating the identity of client companies. The case concerns events that occurred prior to the entry into force of the GDPR, and therefore subject to the regime requiring prior declaration of files containing personal data to the CNIL. The misconduct was established by means of a bailiff's report with the assistance of a computer expert who, using the log files stored on the company's servers, had identified the IP address from which the disputed requests had been sent as being that of this employee. Considering that a prior declaration of the use of log files and IP addresses to the CNIL was not necessary, the Court of Appeal had admitted this evidence as valid and found the dismissal justified. The employee appealed to the Cour de Cassation, arguing that the evidence was unlawful since the processing of logs and IP addresses had not been declared to the CNIL and that the employee had not been informed of such processing operation. The decision of the Cour de Cassation is important for the following reasons: – For the first time in a labour law litigation, the Cour de Cassation states that IP addresses and log files are personal data. – This decision also marks an evolution of the case-law of the Cour de Cassation's Social Chamber regarding the illegality of evidence obtained by means of use of personal data that should have been declared to the CNIL. Indeed, until now, the Social Chamber used to consider that such evidence should systematically be rejected and the dismissal judged without real and serious cause. In the present ruling, the Social Chamber admits that the unlawfulness of such a means of proof should not systematically lead to its rejection, inviting the judge to examine, by carrying out a proportionality review, whether the violation of the employee's personal life caused by the use of such evidence is justified with regard to the employer's right to evidence. The Social Chamber also specified that such production must be indispensable and not only necessary for the exercise of this right (whereas in previous cases it had decided, with regard to other		Explanatory note of the Cour de cassation (in French)

Development	Summary	Date	Links
	unlawful means of proof - e.g. theft of documents by the employee necessary for the exercise of his rights of defence in a dispute with his employer - that such proof was admissible if necessary for the exercise of the rights of defence). This decision also reflects the case-law of the European Court of Human Rights, in particular the Barbulescu case (ECHR, 5 September 2017, No. 61496/08) and Lopez Ribalda case (ECHR, 17 October 2019, nos. 1874/13 and 8567/13) which admitted, on the basis of the right to a fair trial and the resulting right to evidence, proofs obtained at the expense of the right to privacy. After recalling the abovementioned elements, the Cour de Cassation decided in this case that the decision of the Court of Appeal was not justified. In particular, the Court of Appeal had considered that (i) log files and IP addresses constituted computer monitoring that could not be ignored by the employee in view of his position, (ii) it was not subject to declaration to the CNIL, and (iii) should not be the subject of an information notice to the employee in his capacity as DPO, when their primary purpose was not to control employees. It added that only the implementation of a software for analysing the various logs and monitoring user activity had to be declared to the CNIL. Since in the case at issue, it was not a question of implementing such a software but of simply checking the log files, the Court of appeal had considered the evidence against the employee as being valid. Since the Court of Appeal did not consider the evidence to be illicit, when it should have done so in the absence of a declaration to the CNIL and information to the employee, the Cour de Cassation overturned its decision. The Cour de Cassation therefore does not rule on the question of whether such an unlawful piece of evidence could be considered indispensable and proportionate.		
The CNIL imposes penalties on two doctors for breach of health data	On 7 December 2020, the CNIL imposed two fines of €3,000 and €6,000 on two private doctors for failing to adequately protect their patients' personal data and failing to notify a data breach to the CNIL. Following an online check carried out in September 2019, the CNIL found thousands of medical images hosted on servers belonging to the two private practitioners were freely accessible on the Internet.	Date of CNIL's decisions against the doctors: 25 November 2020 Date of CNIL's statement: 17 December 2020	CNIL's decision against the first doctor (in French) CNIL's decision against the other doctor (in French)

Development	Summary	Date	Links
	The CNIL also found that the medical images stored on their servers were not systematically encrypted. The CNIL considered that the two doctors had broken with the basic principles of computer security and failed to comply with the obligation of data security set out in Article 32 of the GDPR. Considering that the doctors should have notified the data breach after finding out that the medical images of their patients were freely accessible on the Internet, the CNIL also considered that there had been a failure to comply with the obligation to notify data breaches set out in Article 33 of the GDPR. Although the CNIL did not consider it necessary to make the identity of the doctors concerned public, it nevertheless wished to ensure the publicity of these decisions in order to raise the awareness of healthcare professionals about their obligations and the need to take security measures concerning the personal data they process.		CNIL statement (in French)
Launch of a public consultation on the standards regarding certification of DPOs	The CNIL can accredit organisations to grant certifications to DPOs on the basis of standards. In order to evaluate these standards, the CNIL has launched a consultation until 6 January 2021. The certification is a voluntary mechanism that allows any professional to demonstrate that he has the professional qualities and knowledge required under Article 37 of the GDPR. The certification is not mandatory to practice as a DPO and it is not required to be appointed as a DPO to apply for the certification. The certificate is a confidence-building tool both for the data controllers using these certified DPOs and for data subjects. Since 20 September 2018, the CNIL has been able to accredit bodies to issue DPO certifications. To date, nine certification bodies have been accredited by the CNIL. This system is based on two complementary standards: – a standard that sets the criteria applicable to organisations wishing to be authorised by the CNIL to certify the DPO's skills, on the basis of the below standard; and	7 December 2020	CNIL statement (in French)

Development	Summary	Date	Links
	– a standard that sets out the conditions for the admissibility of applications and the list of 17 skills and know-how required to be certified as a DPO; These two standards have been in force since September 2018, and provide for a reassessment of their content within two years of their entry into force. The purpose of the consultation launched by the CNIL is to decide whether it is necessary to adapt the requirements set out in the standards. The consultation will end on 6 January 2021.		

Germany

Contributors

Alexander Niethammer
Partner
T: +49 89 54565 318
alexanderniethammer@
eversheds-sutherland.com

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

Ralf-Thomas Wittman
Partner
T: +49 211 86467 17
ralf-thomaswittmann@
eversheds-sutherland.com

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

Steffen Morawietz
Senior Associate
T: +49 89 54 56 52 36
steffenmorawietz@
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
No claim for damages for stolen customer data	A claim for damages for stolen customer data does not exist if the company concerned can prove beyond doubt that the information was taken over without permission. The burden of proof for this lies with the claimant.	1 October 2020	Judgement
Berlin data protection adjustment law - regulatory shortcomings persist	The Berlin commissioner for data protection and freedom of information points out that previous regulatory shortcomings in the Berlin Data Protection Act continue to exist. She calls on the	2 October 2020	Press Statement

Development	Summary	Date	Links
	legislature to remedy these in the course of the announced evaluation of the new Berlin Data Protection Act. The aim of the Berlin Data Protection Amendment Act EU is to adapt a large number of Berlin state laws to meet the requirements of the GDPR, which has been in effect now for over two years. Unfortunately, the legislator has not used this legislative process to remedy major regulatory shortcomings in the Berlin Data Protection Act. The Berlin data protection commissioner sees an urgent need for improvement, especially in the area of data protection supervision and control.		
Data Protection Authority of Hamburg imposes fine of 35,258,708 Euros against H&M	The fashion company with offices in Hamburg operates a service center in Nuremberg. Here, according to the findings of the Hamburg data protection officer, since at least 2014 private details and circumstances of some of the employees have been comprehensively recorded and this information stored on a network drive. For example, the company conducted a "Welcome Back Talk" after employees returned to work after vacation or illness. The information shared in this context - including information regarding symptoms of illness and diagnoses of the employees - was recorded and stored. In addition, according to the Hamburg data protection authority, some supervisors also used the "Flurfunk" [meaning to hear something through the grapevine] to acquire a broad knowledge of individual employees, for example about family problems and religious beliefs. The information stored on the network drive was accessible to up to 50 managers of the company and was used, among other things, to evaluate the work performance of the employees and to make employment decisions.The data collection became known due to a technical configuration error in October 2019, according to which the data stored on the network drive was accessible company-wide for several hours. After the violation became known, the management apologized to the employees and offered monetary compensation. In addition, further protective measures were introduced together with the data protection authority.	1 October 2020	Press Statement
No GDPR damages after data breach	In a civil action following a personal data breach affecting a credit card bonus programme, the Regional Court (Landgericht) Frankfurt am Main rejected claims by a data subject who was affected by the breach for a cease-and-desist injunction and for	1 October 2020	Judgement

Development	Summary	Date	Links
	compensation for non-material damage under Article 82(1) GDPR. The decision is in line with the majority of similar restrictive interpretations of Article 82(1) GDPR by other German courts, requiring evidence of objective harm. Nevertheless, there are also a few more "generous" court decisions favoring a subjective test for proof of non-material damage		
GDPR claim for damages in the amount of EUR 1,000 for unjustified forwarding of data to third parties	As part of an application process, an employee of the controller accidentally forwarded personal data concerning one of the applicants to an uninvolved third party. On the basis of this data protection violation, the Darmstadt Regional Court awarded the data subject damages in the amount of EUR 1,000.	1 October 2020	Judgement
Longer-term storage of a residual debt discharge also under GDPR lawful	The Hamburg Regional Court decided that the long-term storage of the residual debt discharge of a data subject is also lawful under the provisions of the GDPR. Due to a legal interest in the general public under Art. 6 Para. 1 f) GDPR in the storage of this data, the credit agencies are generally only obliged to delete the data after three years of storage. The situation could only change if there was an atypical course of events which justified early deletion. This reason can be of a legal, economic, ethical, social, societal or family nature.	1 October 2020	Judgement
No claim for damages for minor breaches of the GDPR	In its ruling, the Higher Regional Court of Dresden stated that the mere deletion or blocking of a profile in a social network does not automatically give rise to a claim for damages under the GDPR. Rather, more substantial violations are required.	1 October 2020	Judgement
GDPR compensation claims must be given a restrictive interpretation.	As the Regional Court of Frankfurt am Main decided, the claim for damages under Article 82 of the GDPR must be interpreted restrictively. Not every data breach necessarily leads to compensation. Rather, the act of infringement must also have led to a concrete violation of the personal rights of the data subject. A broad interpretation of the concept of damages under Art. 82 GDPR, according to which damages are justified with each violation, contradicts the general approach of German law.	1 October 2020	Judgement

Development	Summary	Date	Links
No claim for damages under the GDPR in the case of minor infringements of the law	It is true that no serious breach of the right of personality is required in order to claim non-material damage. However, not every infringement of the GDPR already leads to an obligation to compensate, because the obligation to compensate for non-material damage must be matched by an identifiable and, in this respect, actual violation of the right of personality, which may lie, for example, in the "exposure" resulting from unlawful access to data.	1 October 2020	Judgement
Data Protection Conference publishes guidance on video surveillance in the private sector	The Data Protection Conference published a guidance document on video surveillance by private parties.	1 October 2020	Guidance
Access by law enforcement authorities to Corona contact lists	The State Commissioner for Data Protection and Freedom of Information of the State of North Rhine-Westphalia published a statement on access by law enforcement authorities to Corona contact lists. The admissibility of access to the Corona contact lists by the criminal prosecution authorities in the context of criminal investigations is governed in particular by the Code of Criminal Procedure (StPO). As soon as the police become aware of an initial suspicion of a crime, they are obliged to investigate the facts of the case in accordance with the principle of legality. According to the so-called general investigation clause of § 163 StPO, the police are authorised to conduct investigations of any kind. The same applies to the public prosecution authorities. This means that the police and the public prosecutor's office may in principle conduct all investigations which do not require special powers of intervention due to the intensity of their encroachment on fundamental rights. Such an increased encroachment on fundamental rights cannot regularly be assumed when accessing the Corona contact lists. Therefore, access to guest lists on the basis of the general investigation clause is possible in principle. However, access to the corona contact lists must also be necessary and proportionate for the investigations.	1 October 2020	Press Statement
Decision of Data Protection Conference on competence of the court of first instance for data breaches	With the "Draft Law on the Effectiveness of Fines Proceedings", the Federal Council intends to abolish the jurisdiction of the regional courts of first instance for fines exceeding 100,000 euros under the General Data Protection Regulation (GDPR). Even fines of this amount will in future be decided by the local courts.	1 October 2020	Decision

Development	Summary	Date	Links
	However, the planned law will not achieve the objective of making the fine proceedings more effective. The draft law blatantly ignores the particular economic, technical and legal complexity of GDPR fines. Moreover, a deletion of the regional court's jurisdiction would not relieve the local courts of their workload, but would instead place an even greater burden on them than at present. The Conference of the Independent Data Protection Supervisors of the Federal Government and the States (Data Protection Conference) therefore calls for the retention of the jurisdiction of the regional courts for GDPR fines exceeding EUR 100,000 and warns against a deletion of the provision and its consequences.		
Hospital must give patient access to medical treatment data free of charge.	The court in Dresden ruled that a hospital patient must be given access to his medical treatment data free of charge. Insofar as the data subject relies on Article 15(3) of the GDPR to substantiate his right to access, there are consequently no grounds to claim for the costs of compiling and transmitting the data. The initial information should be free of charge.	1 October 2020	Judgement
No claim for damages under GDPR for unauthorised banning on a social media platform	If a social media platform blocks a user without justification due to an allegedly illegal contribution, there is no claim for damages for him or her under Art. 82 GDPR. For this to happen, there would first have to be a relevant violation of data protection, which is not usually the case. In addition, the data subject must have suffered damage, which is rarely assumed in such circumstances.	1 October 2020	Judgement
The right of access according to Art. 15 GDPR does not include e-mails	A former employee brought a claim for access in accordance with Art. 15 GDPR against his former employer after his dismissal and demanded, among other things, to receive a copy of all e-mails he had written during his professional activity. The Regional Labour Court rejected the claim as unfounded on the basis that the data subject had written the messages himself, and the content was therefore known to him. In view of the wording of Article 15(3) of the GDPR, which speaks only of data which is ""subject to processing"", a certain degree of information about the data subject must be required. This also follows from Recital 63 to the DSGVO. According to this recital, where the controller processes a large amount of information	1 October 2020	Judgement

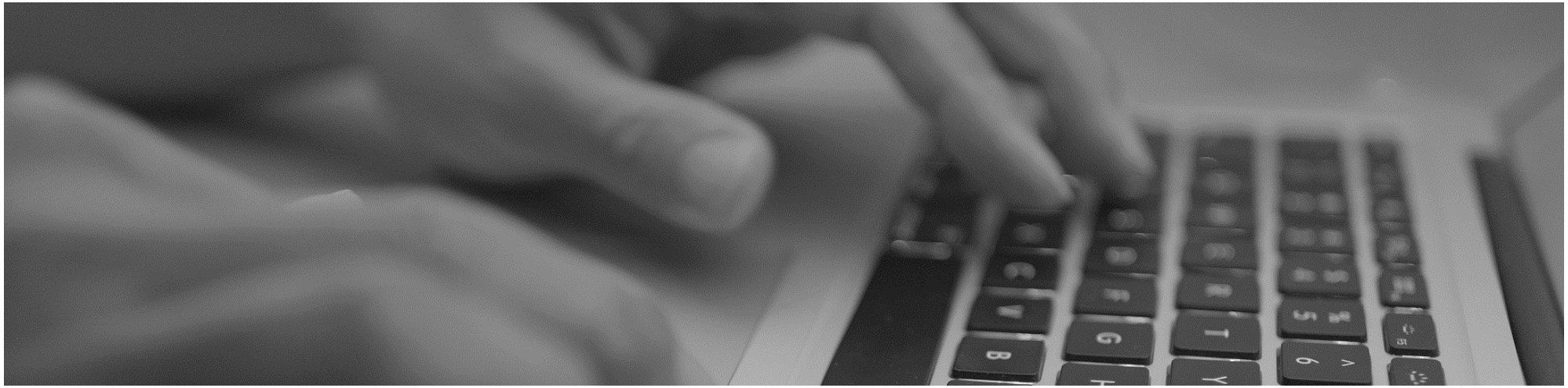
Development	Summary	Date	Links
	relating to the data subject, he may require the data subject to specify to which information or which processing operations his data access request relates before providing the information. In addition, the right of access is limited to those documents which are not already available to the person requesting information. As such, the Court requires that data subjects specify in more detail their general data access request in relation to specific documents and to give reasons, inter alia, why they do not already have the document in question. The purpose of the provision of access and the making available of a copy is to enable data subjects to verify the data processing, but not to obtain complete copies of all documents containing personal data relating to them.		
Claim for damages in the amount of EUR 1,500 in the event of unauthorised disclosure of health data	After his employer unlawfully disclosed data on his state of health to the foreigners authority and employment agency, a data subject was granted a GDPR compensation for damages in the amount of EUR 1,500 in accordance with Art. 82 GDPR. According to the Labour Court of Dresden, this amount is necessary but also sufficient to compensate for the non-material damage.	1 October 2020	Judgement
The Federal Commissioner for Data Protection and Freedom of Information critisizes Source Telecommunications Surveillance for Messaging Services	The Federal Commissioner of Data Protection and Freedom of Information criticizes the German government's plans to allow the intelligence services to monitor messengers. The existing legal situation is not ready for the introduction of such massive encroachments on privacy: ""The courts have shown a clear need for reform in the laws governing the intelligence services. Instead of tackling these urgent reforms, new surveillance options are now to be created. I call once again for a moratorium on security laws and an independent scientific analysis of existing laws"".	23 October 2020	Press Statement
No GDPR compensation claim in the event of a one-off incorrect sending of account statements by the house bank	A one-off and first-time sending of a bank statement comprising a few sheets of paper to the wrong recipient. In the view of the Cologne Regional Court, this is a simple minor infringement which does not justify compensation for damages. Otherwise, there would be a risk of unlimited liability for the economy, which cannot correspond to the meaning and purpose of Art. 82 GDPR. In its overall assessment, the Court of First Instance took into	7 October 2020	Judgement

Development	Summary	Date	Links
	account, in the light of the criteria laid down in Article 83(2) of the GDPR, the fact that the data subject considered the present case to be subjectively very onerous. However, the Court nevertheless considered that, overall, the award of damages for pain and suffering was not justifiable.		
Data protection authority may not order the removal of unlawful video surveillance	An entrepreneur had installed several video cameras to protect his valuable billboard. The data protection officer of Rhineland-Palatinate classified this as a violation of the GDPR, prohibited further operation and ordered, among other things, the removal of the cameras. Administrative Court Mainz held that the data protection authority was not entitled to make this order. Article 58(2)(f) GDPR allows the supervisory authority to restrict or even prohibit data processing temporarily or permanently. However, this legal basis does not include the ability to order the removal of the processing system. The prohibition of data processing relates to a specific act, but not to the presence of a data processing system which has been switched off. Particularly noteworthy are the Court's comments on the processing of personal data of special categories within the meaning of Article 9 of the GDPR, as would be possible by means of video surveillance: "*By means of video surveillance, the controller intends to prevent and prosecute criminal offences. With the surveillance, he receives a mixed data set of particularly sensitive and non-sensitive data, whereby he has no intention of processing the sensitive data. In the absence of such a processing intention, there are no particular risks for the persons concerned, so that the scope of application of Art. 9 para. 1 GDPR is not triggered*". Consequently, the mere theoretical processing possibility is no longer taken into account, but the intention of the controller. It is questionable whether this opinion will also be confirmed by other courts.	1 October 2020	Judgement
Court rules that data subject has a GDPR claim against data protection authority to enforce right to erasure against Google	Various statements were made about a data subject in an Internet forum. However, the data subject was unable to assert claims against Google directly in court and therefore turned to the Hamburg data protection commissioner and requested official intervention. The authority refused to do so. Consequently, the	7 October 2020	Judgement

Development	Summary	Date	Links
	data subject brought an action before the Dresden Higher Administrative Court. In the course of the proceedings, the court made it clear that every data subject has a GDPR right against the data protection authorities to intervention without any discretionary error.		
Comprehensive right of action by data subjects in case of GDPR infringements	The Frankfurt Regional Court assumes that a data subject can also assert claims under data protection law by way of injunction and that such claims are not blocked by Art. 79 GDPR. The objective of the GDPR is to enable the data subject to assert his claims as widely as possible.	15 October 2020	Judgement
Test scheme of data protection authorities for companies to transfer data under Schrems II	In order to provide controller and processors with practical support in implementing the Schrems II judgement, the State Commissioner for Data Protection and Freedom of Information of the State of Rhineland-Palatinate has prepared an overview with individual test steps. On the basis of the guide, data controller can approach individual solutions for the data protection-compliant transfer of personal data to third countries. The test scheme also refers to further information on individual questions.	11 November 2020	Test Scheme
Examination of cookies and third-party services on Lower Saxony websites	Companies in Lower Saxony use cookies on their company websites rather sparingly, but at the same time they do not inform users enough about the data collected when they visit their sites. This is the result of a cross-industry audit by the State Commissioner for Data Protection of Lower Saxony on data protection-compliant tracking on websites. For this purpose, the Commissioner had sent a questionnaire to 15 small and medium-sized enterprises that offered one or more websites.	25 November 2020	Press Statement
GDPR right to information also includes mere telephone memos	In its decision, the Regional Court of Cologne confirmed that the right to information under Art. 15 GDPR is to be understood comprehensively and also covers bare conversation notes and telephone memos.	11 November 2020	Judgement
Mention of a company employee by name in online rating not a GDPR violation	In an online Google review, a user wrote a critique about a company and explicitly mentioned the name of an employee. Google was asked to delete the name with reference to the GDPR, but the search engine provider did not react.	29 October 2020	Judgement

Development	Summary	Date	Links
	The court ruled that there was no right to deletion. This is because the naming is justified by the right to freedom of expression. Not every mention of a name constitutes a violation of data protection and an unjustified encroachment on the personal rights of the person concerned. Rather, a balancing of the concerned interests must take place.		
EUR 300.00 GDPR damages for a forgotten online PDF file	If an employer fails to delete a PDF containing personal data of an employee after the employee has left the company, this is a GDPR violation and justifies damages of EUR 300.	1 October 2020	Judgement
The majority of German cookie banners are unlawful	The court ruled that most cookie banners on German websites are faulty and thus illegal. The defendant company had designed its homepage in such a way that a cookie banner appeared when it was called up. There were four smaller pre-activated menu items: ""[ ] Necessary [ ] Preferences [ ] Statistics [ ] Marketing"". In addition, there was the item ""Show details"" and a larger, green-bordered and visually highlighted ""OK"" button. The district court found this to be clearly against the law because no informed consent was obtained from the user. Although the consumer has the option to view the details and to deselect individual cookies. In fact, however, the consumer will regularly avoid the effort of such a procedure and therefore press the button without prior information about the details. In this way, the consumer does not know the consequences of his consent. The Regional Court also found the colour highlighting of the consent button to be unlawful, as it overshadowed the other button.	1 October 2020	Press Statement
No GDPR damages for only insignificant infringements	In the case of only minor, insignificant breaches of the law, no GDPR damages under Art. 82 GDPR can be considered. In any case, the infringing act must also have led to a concrete, not merely insignificant or perceived infringement of the data subject's data privacy rights.	6 November 2020	Judgement
Data subject has no GDPR claim against data protection authority for certain actions	The court considers that a data subject does not have a GDPR claim against a data protection authority for certain actions. In particular, he or she does not have the right to have the content of the decision in question judicially reviewed for its correctness.	26 October 2020	Judgement

Development	Summary	Date	Links
	Rather, the GDPR only grants the data subject a simple right of petition. Rather, a data subject can only claim against an (inactive) supervisory authority that the authority deals with his or her complaint at all and informs him or her about the status and the result of the complaint within the specified time periods.		
Requirement to use a real name on social media not legally objectionable	Users can be required to state their real name (or "clear name") when using a social media platform. The use of pseudonyms, on the other hand, can be prohibited. The court agreed that requiring clear name to help prevent cyber bullying, harassment, insults and hate speech, is within a company's legitimate interest to protect its users.	8 December 2020	Judgement



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

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

Yikai Sit
Trainee Solicitor
T : +852 9736 8790
yikaisit@
eversheds-sutherland.com

Jenny Chen
Trainee Solicitor
T: +852 2186 4984
jennychen@
eversheds-sutherland.com

Development	Summary	Date	Links
First doxxing case convicted and sentenced for contravention of the Personal Data (Privacy) Ordinance (Chapter 486 of Laws of Hong Kong) (the "PDPO")	In a recent case (DCCC 164/2020), a telecommunications technician who through his position in a telecommunications company obtained the personal data of a family member of a police officer and disclosed it on social media was convicted, among others, of an offence under section 64(2) of the PDPO. Under section 64(2) of the PDPO, a person commits an offence if he discloses, irrespective of his intent, any personal data of a data subject obtained from a data user without the data user's consent and the disclosure causes psychological harm to the data	3 November 2020	PCPD Media Statement

Development	Summary	Date	Links
	subject. The Defendant was sentenced to an imprisonment of 18 months under this conviction alone and to a total of 24 months' imprisonment together with other convictions. This is the first doxxing case where the defendant has been convicted and sentenced to imprisonment for contravention of the relevant requirements since section 64(2) of the PDPO was amended in 2012. Contravention of section 64(2) of PDPO leads to serious criminal liabilities. On conviction, the maximum penalty is a fine of HK$1,000,000 and imprisonment for 5 years. If relevant doxxing cases involve criminal elements, including possible contravention of section 64 of the PDPO, the Office of the Privacy Commissioner for Personal Data, Hong Kong, (the **"PCPD"**) will refer such cases to the police. By the end of October 2020, the PCPD had referred over 1,400 cases to the police for further investigation and consideration of prosecution, and the police arrested 13 persons for potential contravention of section 64 of the PDPO concerning the disclosure of personal data obtained without the consent from relevant data users.		
Hong Kong Monetary Authority (the "HKMA") launched Cybersecurity Fortification Initiative 2.0	Following extensive industrial consultation and a review of the existing Cybersecurity Fortification Initiative, which was launched in 2016 to raise the cyber resilience of Hong Kong's banking system, the HKMA has recently announced the launch of the enhanced Cybersecurity Fortification Initiative 2.0. The Cybersecurity Fortification Initiative is underpinned by three pillars – the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP) and the Cyber Intelligence Sharing Platform (CISP). Cybersecurity Fortification Initiative 2.0 has introduced a series of enhancement measures. Among other things: – recent international sound practices on cyber incident response and recovery have been incorporated into the enhanced control principles under the C-RAF; – the certification list for the PDP has been expanded to include equivalent qualifications in major overseas jurisdictions; and	3 November 2020	HKMA's Circular on Cybersecurity Fortification Initiative 2.0 Annex to the Circular

Development	Summary	Date	Links
	– the HKMA has put forward a series of recommendations to the Hong Kong Association of Banks to make the CISP more user-friendly. The Cybersecurity Fortification Initiative 2.0 came into effect on 1 January 2021. The HKMA adopts a phased approach to implementation, dividing authorised institutions into three groups, with different timeframes for completing the C-RAF assessments. Implementation by all groups is expected to be completed by end of 2023.		
Office of the Privacy Commissioner for Personal Data, Hong Kong, (the "PCPD") issued three practical Guidance Notes relating to work-from-home arrangements for (1) organisations, (2) employees and (3)users of video conferencing software	Due to COVID-19, work-from-home arrangements have become a new normal for many people. In light of the new risks posed to data security and personal data privacy as a result of work-from-home arrangements, PCPD issued three Guidance Notes under the series "Protecting Personal Data under Work-from-Home Arrangements" to provide practical advice to (1) organisations, (2) employees, and (3) users of video conferencing software to enhance data security and the protection of personal data privacy. In the Guidance Note, the PCPD recommends that organisations should: – set out clear policies on the handling of data during work-from-home arrangements; – take all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate work-from-home arrangements, or when data and documents are transferred to employees to work from home; – provide sufficient training and support to their employees under work-from-home arrangements; and – ensure the security of the data stored in the electronic devices provided to employees. The PCPD recommends that employees should: – adhere to their employers' policies on the handling of data;	30 November 2020	PCPD Media Statement Guidance for Organisations Guidance for Employees Guidance on the Use of Video Conferencing Software

Development	Summary	Date	Links
	– use only corporate electronic devices for work as far as practicable; – enhance the security of Wi-Fi connections and electronic communications; – avoid working in public places to prevent accidental disclosure of personal data or restricted information to third parties; and – ensure proper handling of data when it is necessary to take paper documents out of office premises. In relation to the use of video conferencing software, the PCPD recommends that users should: – review and assess the policies and measures on the security and protection of personal data privacy of different video conferencing software in order to choose the ones that meet their needs; – safeguard their user accounts by setting up strong passwords, changing the passwords regularly, and activating multi-factor authentication; and – verify the identities of the participants of video conferences to prevent unauthorised access.		

Hungary

Contributors

Ágnes Szent-Iványi
Partner
T: +36 13 94 31 21
szent-ivany@
46versheds-sutherland.hu

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

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

Development	Summary	Date	Links
Resolution of the NADP No. NAIH/2020/66/21 on the design and the operation of the travel agency's website and the privacy incident affecting it	The Authority imposed a fine of HUF 20,000,000 (~EUR 55,700) on a travel agency, as data controller. The data controller entrusted the design of its website to an improperly selected data processor, which led to serious infringement and data management planning deficiencies. It used and operated its system and website for the storage of personal data managed in connection with the offered travel services in such a way that anyone could access it via the Internet. Due to this deficiency, the confidentiality of the data was seriously compromised. The travel agency failed to inform the data subjects of this breach, thus failing to comply with its obligations. The Authority also imposed a fine of HUF 500,000 (~EUR 1,400) on the data processor. During the operation of the website, the data processor did not terminate the connection between the test database and the live database and did not subject the website to appropriate security checks and vulnerability tests.	9 December 2020	NADP resolution
Guidance of the NADP No. NAIH/2020/7465 concerning certain data processing operations related to the measurement of	In its Guidance NAIH/2020/2586 on 10 March 2020 concerning data processing operations related to the coronavirus epidemic, the Authority stated that in view of the epidemiological situation in Hungary at the time, it did not regard the requirement of health	13 October 2020	NADP Guidance

Development	Summary	Date	Links
body temperature during the period of epidemiological readiness introduced with ordering a health emergency in view of the novel coronavirus pandemic (Covid-19)	care data processing associated with the use of diagnostic instruments and the introduction of mandatory screening for body temperature as proportionate, and hence it was not deemed in compliance with the data protection principles. However, in view of the continuously and significantly increasing number of cases, the Authority arrived at the conclusion that the use of diagnostic screening devices related to the measurement of body temperature during the current phase of the novel coronavirus epidemic in connection with community spread and mass infections qualifies as being in compliance with the principles provided that the following conditions are met: – it is used in the course of allowing entry to the area or buildings owned or used by the controller; – it is used as a protective measure uniformly with every person desiring to enter ("**shell protection**"); – it is not linked to the identification of the subject of the body temperature check expressly to achieve this processing purpose, and it does not involve the recording, storage, or transmission of data in any way.		

Ireland

Contributors

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

Development	Summary	Date	Links
DPC replies to representation received from Senator Malcolm Byrne on 7 October 2020	The DPC has replied to a representation received from Senator Malcolm Byrne saying they will not be covering the cost of the Schrems II case. In their response, the DPC considers that the defendant, and not the DPC, should pay the complainant's costs.	10 October 2020	DPC Guidance
DPC issues statement on funding in 2021 budget	The DPC has issued a statement welcoming the allocation of €19.1 million in funding, as announced by the Government in Budget 2021.	13 October 2020	DPC Guidance
DPC issues two statutory inquiries into processing of children's data on social media (opened in September 2020)	The DPC has identified potential concerns in relation to the processing of children's personal data on social media which requires further examination. The first inquiry will assess the legal bases for processing of child personal data on the platform. The second inquiry will focus on profile and account settings and the appropriateness of these settings for children.	19 October 2020	DPC Guidance
DPC fine on Tusla Child and Family Agency confirmed in court	This update relates to three personal data breaches notified by Tusla to the DPC. All three breaches occurred in circumstances where Tusla failed to redact personal data when providing documents to third parties. The DPC imposed an administrative fine of €75,000	4 November 2020	DPC Guidance
DPC provides guidance on EU-US Data Transfers – Judicial Review Proceedings	The DPC has published a press release which provides details relating to Facebook's judicial review proceedings against the	3 December 2020	DPC Guidance

Development	Summary	Date	Links
	DPC. These proceedings are listed for hearing in the Irish High Court on 15 December 2020. Facebook's central complaint is that, in commencing the inquiry, and in issuing the Preliminary Draft Decision, the DPC has not respected Facebook's right to fair procedures.		
DPC announces decision in Twitter inquiry	The DPC has announced that Twitter has infringed Articles 33(1) and 33(5) of the GDPR in terms of a failure to notify a GDPR breach on time to the DPC and a failure to adequately document the breach. The DPC has imposed an administrative fine of €450,000 on Twitter.	15 December 2020	DPC Guidance
DPC issues guidance on the fundamentals for a child-orientated approach to data processing	This guidance discusses the DPC's recently drawn up fundamentals for a child-orientated approach to data processing. Specifically the introduction of child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of / access to services in both an online and offline world.	18 December 2020	DPC Guidance
DPC prepares Language Scheme for 2020-2023	The DPC has prepared its fifth Language Scheme in accordance with section 15 of the Official Languages Act 2003. The scheme shall remain in force for a period of 3 years from 21 December 2020 or until a new scheme has been approved, whichever is the later.	21 December 2020	DPC Guidance
DPC issues guidance on transfers of personal data from Ireland to the UK at the end of the transition period (11pm on 31 December 2020)	This DPC Guidance maintains that Irish based data exporters can continue to transfer the personal data to UK based data importers after the end of 2020 without the requirement to apply additional safeguards such as Standard Contractual Clauses, administrative arrangements or other appropriate safeguards outlined in Chapter V of the GDPR.	31 December 2020	DPC Guidance

Italy

Contributors

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

Andrea Zincone
Partner
T: +39 06 893 2701
andreazincone@
eversheds-sutherland.it

Development	Summary	Date	Links
Italian Data Protection Authority ("IDPA") guide on the usage of Apps	The IDPA published a new section of its website dedicated to the usage of Apps, including a guide on the usage of Apps with a view to protect personal data.	30 October 2020	IDPA's website page on Apps (only available in Italian language)
IDPA fined a telecommunications operator more than Euro 12 millions	The IDPA has fined a primary telecommunications operator more than €12 million for unlawfully processing personal data of millions of users for telemarketing purposes. The IDPA also required the operator to implement several measures in order to comply with Italian and EU data protection law. This decision is the outcome of complex proceedings that IDPA had initiated following hundreds of complaints and alerts submitted by users regarding unsolicited phone calls made by the operator and/or its sales network in order to promote telephone and Internet services. The investigations carried out by the IDPA highlighted major inadequacies regarding the operator's consent requirements and compliance with accountability and data protection by design principles. The IDPA found that these inadequacies covered both processing activities performed in respect of the operator's customer database and with regard to prospective users of electronic communications services. The IDPA's investigations highlighted the use of fake telephone numbers or numbers that were not registered with the ROC (the National Register of Communication Operators) in order to place the marketing calls. The IDPA found additional violations regarding the handling of contact lists purchased from external providers and transferred to	Date of the IDPA's measure: 30 October 2020 Date of the IDPA's press release communicating the measure: 16 November 2020	The IDPA's measure n. 224 of 12 November 2020 (only available in Italian language) IDPA's press release

Development	Summary	Date	Links
	the operator without the users' free, informed, and specific consent. The IDPA also deemed that the operator's customer resource management and security measures were inadequate. The IDPA received several complaints and alerts from customers who had been contacted by third parties on the operator's behalf, requesting IDs to be sent to them via WhatsApp. Finally, the IDPA has prohibited the operator from performing processing activities for marketing or commercial purposes where data is acquired from third parties that have not obtained the users' free, specific, and informed consent to data disclosure.		
IDPA's guide on the publication of pictures online	The IDPA made available a section of its website dedicated to the publication of pictures online. This section includes a guide providing suggestions to protect personal data.	24 November 2020	IDPA's website page (only available in Italian language
IDPA's FAQs on video-surveillance	The IDPA has published its FAQs regarding video-surveillance and the deployment of CCTV systems. These FAQs provide general guidance on the topic. The IDPA makes explicit reference to the EDPB's Guidelines 3/2019 on the processing of personal data through video devices, and states that there is no need for a specific authorisation to deploy a CCTV system. In particular, the IDPA highlights the need to provide data subjects with appropriate information pursuant to the GDPR. With this in mind, the IDPA has provided a template for a simplified information notice, to be supplemented by a complete notice setting out all of the GDPR requirements. The IDPA emphasises the need to comply with data protection principles; in particular, the principles of data minimisation and storage limitation. The IDPA does not prescribe specific data retention periods, but recommends applying the shortest ones possible, taking into account any retention obligations under the applicable law, and the actual need to record footage (the IDPA provided an example default period of 24-72 hours, but generally speaking, the longer the retention period is, the stronger the justification that will be required). The IDPA also remarks that these FAQs are without prejudice to the requirement to perform a Data Protection Impact Assessment	5 December 2020	IDPA's press release making FAQs available (only available in Italian language) IDPA's FAQs on video-surveillance (only available in Italian language)

Development	Summary	Date	Links
	and to the requirements under Italian employment law, where cameras may film employees.		
IDPA's public consultation on guidelines regarding cookies	The IDPA published new guidelines regarding cookies and their usage (including an annexed summary sheet) for consultation. These guidelines are an update on the previous IDPA's measures (dated 2014 and 2015) following the implementation of GDPR and of the most recent developments of this matter. The IDPA has included guidance on matters such as: consent requirements according to the GDPR; the acquisition of consent and "scrolling" practices; the prohibition of cookie-walls; the repetition of consent requests; the provision of appropriate information notices; and the usage of third-party cookies.The guidelines were published on the Italian official Journal on 11 December 2020. The consultation was open for 30 days following publication.	Date of press release announcing the public consultation: 5 December 2020 Date of measure: 26 November 2020	IDPA's press release announcing the public consultation on cookie guidelines (only available in Italian language) IDPA's measure providing cookie guidelines and the summary sheet (only available in Italian language)
IDPA's guide on the right of access	The IDPA recently produced a guide on the right of access. This is the first of a series of guides concerning rights under the GDPR, to be published on IDPA's website.	17 December 2020	IDPA's website information page on rights (only available in Italian language)
IDPA published a new online service regarding the notification of data breaches	The IDPA has published an online self-assessment tool to help controllers better identify cases of data breaches and proceed with the relevant notification. The IDPA also published template notification forms and an information guide.	23 December 2020	IDPA's website page (only available in Italian language)
IDPA's guide on deepfakes	The IDPA has also made published a dedicated page of its website regarding "deepfakes" and the relevant risks.	28 December 2020	IDPA's website page (only available in Italian language)

Lithuania

Contributors

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

Development	Summary	Date	Links
The State Data Protection Inspectorate has prepared guidelines on customised and standardised data protection	The State Data Protection Inspectorate has prepared guidelines regarding the "Customised and standardised data protection in the life cycle of an information system". These guidelines will help controllers and processors of personal data understand and comply with the requirements of data protection by design and default, as provided for in Article 25 of the GDPR during the life cycle of the information system. The guidelines are intended for developers of information systems or individual software, information technology project managers, information technology architects, programmers, testers, data protection officers and other persons involved in the development of information systems that process personal data. The life cycle of an information system includes all changes in the state of the system from its creation to the end of its operation, i.e. information system initiation, development, operation, modernization, liquidation. Among other things, the life cycle thinking in the guidelines also applies to individual software or hardware development.	15 December 2020	Guidelines (in Lithuanian)
The State Data Protection Inspectorate has prepared "Guidelines for the Assessment of Requests for the Provision of Personal Data"	The State Data Protection Inspectorate, having considered the requests of data controllers and data processors regarding the lawfulness of incoming requests for personal data ("**Access Requests**") and the criteria for assessing whether the Access Requests can be satisfied, has developed guidelines for the assessment of Access Requests for the Provision of Personal Data ("**Guidelines**"). The main topics in the Guidelines are:	11 November 2020	Guidelines (in Lithuanian)

Development	Summary	Date	Links
	– Evaluation criteria for the provision of personal data. The Guidelines address the assessment of the legality and reasonableness of the Access Requests, which is based on three main criteria: the lawfulness of the purpose, the suitability of the recipient and the proportionality of the amount of personal data requested to the purpose of the Access Request; – Conditions for the processing of lawful personal data. The Guidelines specify the application of all the conditions for the lawful processing of personal data laid down in Article 6 of the GDPR and the related responsibilities of the controller; – Cases where the GDPR does not apply, i.e. personal data of the deceased (with exceptions), data of legal persons, and anonymized information is requested; – Provision of personal data to law enforcement authorities. The Guidelines discuss recommendations for the content of law enforcement requests; and – Provision of personal data to attorneys. The Guidelines discuss the conditions under which attorneys' Access Requests could be based on the processing of lawful personal data, and the basis for rejecting such requests.		
"ADA Gidas" is a new mobile app for disseminating information about personal data protection	The mobile app "ADA Gidas" was developed by the State Data Protection Inspectorate and Mykolas Romeris University to promote high standards of personal data protection and increase awareness in the field of personal data protection as part of the SolPriPa project, co-financed by the European Union Program on Rights, Equality and Citizenship (2014-2020). It is intended to disseminate the results of the project and to promote public awareness of the personal data protection supervision activities carried out by the State Data Protection Inspectorate, and in some cases even to contribute to it. The SolPriPa project develops information published in an "ADA gidas" for organisations and individuals, in particular health care providers, start-ups, small and medium-sized enterprises, the media, young people, and the elderly. Device information will be updated, and new topics added in the future. The "ADA gidas" mobile application includes special sections with useful	28 October 2020	

Development	Summary	Date	Links
	information for organisations and individuals, information in English, collated BDAR texts in Lithuanian and English, surveys, tests, and a "your opinion" section. Through the app, organisations will also be able to complete a test to assist them in determining whether a particular personal data breach should be reported to the State Data Protection Inspectorate. In addition, the app provides an opportunity to anonymously share your assessments and insights on personal data processing and report concerning personal data processing in the market, thus helping the State Data Protection Inspectorate to carry out personal data protection supervision activities, monitor the situation in Lithuania, assess emerging risks, and plan inspections.		

Mauritius

Contributors

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

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

Renand Pretorius
Senior Associate
T: +230 211 0550
renandpretorius@
eversheds-sutherland.mu

Zaafir Raymode
Associate
T: +230 211 0550
zaafirraymode@
eversheds-sutherland.mu

Development	Summary	Date	Links
Can Global Business Entities lawfully dispense from registration as a Controller with the DPO?	In line with recent communications between the Data Protection Office (the **"DPO"**) and the Association Trust & Management Companies (the **"ATMC"**), recent updates highlight that the blanket exemption that previously allowed all GBC/GBL and Authorized Companies to rely on their respective management companies to dispense with the need to register as Controller with the DPO, is no longer applicable (the **"Communications"**). Prior to the Communications, a management company could register on behalf of a global business entity when the management company kept all the personal data of the said global business entity (i.e. when all the personal data are centralised at the management company). Following the Communications, a more stringent subjective test will need to be applied to companies under management to ascertain whether they will be required to register independently with the DPO. The new test allows that a management company can only register as a controller on behalf of a global business entity where: – all the personal data is centralised with the management company;	8 October 2020	

Development	Summary	Date	Links
	– the decision making powers, with respect to the processing of personal data, rest solely under the management company; and – it is solely the management company who can determine the purposes and means of the processing of personal data. Example 1: Must a global business register as a controller with the DPO when it a operates independently and its management company is merely acting as company secretary? Answer 1: If the global business makes decisions with respect to the purposes for which and in the manner in which personal data (employees or non-employees) are, or are to be, processed, then it is likely that the global business must register itself as a controller with the DPO. Example 2: Must a global business register as a controller with the DPO where a commercial operation is carried out directly by it? Answer 2: It is likely that the global business will have to register as a controller with the DPO since it will be assumed that personal data are not not centralised with its management company.		

Netherlands

Contributors

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

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

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

Marijn Rooke
Associate
T: +31 6 3026 1891
marijnrooke@
eversheds-sutherland.com

Sarah Zadeh
Associate
T : +31 6 8188 0484
sarahzadeh@
eversheds-sutherland.com

Development	Summary	Date	Links
The DDPA issues warnings on the meaning of article 58 (2)(a) GDPR to a supermarket for the use of facial recognition software and the processing of biometric data	On 15 December 2020, the Dutch Data Protection Authority ("**DDPA**") issued a warning on the meaning of article 58(2)(a) GDPR. The DDPA imposed the warning on a supermarket that used CCTV in the shop. By means of the CCTV at the entrance of the shop, everyone who entered the shop was (for a short period of time) registered and the faces of visitors were then compared with a database of faces of people who had previously been banned from entering the shop. The faces of people without a ban were deleted after a few seconds. The supermarket said it used facial recognition to protect shop visitors and staff and to prevent shoplifting. Following signals in the media, the DDPA requested information from the owner of the supermarket on 6 December 2019. On 8	15 December 2020	DDPA Statement (in Dutch)

Development	Summary	Date	Links
	December 2019, the supermarket switched off the facial recognition system. However, in the documents provided to the AP, the owner of the supermarket stated that he wished to reactivate the system. That is why the DDPA intervened. Facial recognition uses biometric data to identify a person. Biometric data is a special category of personal data. The processing thereof is prohibited in the Netherlands, except for two exemptions: – First, that the people being filmed have given their express consent. According to the supermarket owner, customers were warned that the supermarket was using facial recognition. However, according to the DDPA, this does not constitute explicit consent. – 2. Second, the other exception, laid down in article 29 of the Dutch GDPR Implementation Act ("**UAVG**"), is if facial recognition is necessary for authentication or security, but only where there is an overriding public interest. The supermarket was of the opinion that this applied but the DDPA did not agree with this interpretation. The Explanatory Memorandum to article 29 UAVG mentions the security of a nuclear power station as the only example. Thus, the bar is high and preventing shoplifting is very different from preventing a nuclear disaster, according to the DDPA. Since neither of the two exceptions to the legal ban on processing biometric data applies, the DDPA finds that the proposed processing is unlawful. The DDPA therefore imposes a formal warning in order to prevent the supermarket from using the facial recognition software again.		
Dutch Council of State considers DSAR (article 15 GDPR) – which primarily aims for compensation (article 82 GDPR) of damages – in line with GDPR	On 9 December 2020, the Dutch Council of State rendered a ruling on appeal regarding a data subject access request (DSAR). By a decision of on 2 January 2018, the Municipal Executive of the municipality Zundert denied the request of the data subject to access his personal data. According to the data subject, the personal data had been processed for, among other things, requests submitted earlier pursuant to the Government Information (Public Access) Act (Wob). He had also requested that, insofar as the Municipal Executive processed his personal	9 December 2020	Court Ruling (in Dutch)

Development	Summary	Date	Links
	data by posting messages on the forum of the Association of Netherlands Municipalities (VNG), the contents of these messages be included in the overview. Finding out which municipalities had posted the data subject's personal data on the VNG forum is in line with the purpose of the GDPR, however, in this instance, a request to access the VNG did not make sense because the data had been removed. The data subject hoped that the Municipal Executive made screenshots of the forum or was able to find out in some other way what was posted on the forum. He also requested compensation/damages if the Municipal Executive was found to have processed personal data unlawfully, which is possible under the GDPR. The court found that the fact that a claim for compensation would be the underlying purpose of this DSAR, and also of the other DSAR's that the data subject had submitted, does not mean that the purpose of the DSAR is no longer in line with the purpose of the GDPR.		
The DDPA investigates two large companies that measured the temperature of employees during COVID-19 crisis	The DDPA has investigated two large companies that measured the temperature of their staff as a result of the COVID-19 outbreak. The DDPA found that both companies, including a multinational company, had acted in violation of the GDPR. In the Netherlands, health data of employees may only be processed by the company doctor or another medical professional that has been contracted by the employer. The DDPA has taken a strict stance regarding the processing of health data by employers, despite the current COVID-19 crisis. Based on their investigations, the DDPA concluded that the two companies had processed health data of their employees, as these companies processed the body temperatures of their employees. In the Netherlands, body temperature that can be related to an individual is considered to be health data, and thus special category data, one of the exemptions as mentioned in article 9(2) GDPR must apply. Initially, one of the employers relied on the consent exemption of article 9(2)(a) GDPR. However, the DDPA stated that due to the power-imbalance between an employer and an employee, an	26 November 2020	DDPA Statement (in Dutch)

Development	Summary	Date	Links
	employer cannot rely on consent to process the health data of employees. The DDPA has urged both companies to improve matters. In the near future, the DDPA will check the companies again to determine whether the way in which temperatures have been adjusted.		
The District Court Midden-Nederland rules in first instance that an 'exclusively commercial interest' may be a legitimate interest in the meaning of article 6 (1)(f) GDPR	On 23 November 2020, the District Court Midden-Nederland ruled in first instance that an 'exclusively commercial interest' may constitute a legitimate interest within the meaning of article 6(1)(f) GDPR. This case concerned an internet platform on which amateur football matches are broadcast. The DDPA imposed a fine of €575,000 on the basis that there was no legal basis for recording and broadcasting such football matches (and thus processing personal data). The production and processing of recordings is an invasion of the privacy of a large number of individuals concerned and, because underage football players were involved, justified a significant fine. The platform responded by initiating administrative court proceedings against the DDPA. Notably, at this point the platform had already gone bankrupt. The decision to impose a fine was issued a long time after the conclusion of the investigation (report) and the users of the platform had largely abandoned it, due to the uncertain outcome in the meantime. According to VoetbalTV, the recording and broadcasting of football matches falls within the scope of the journalistic exception; an argument which the Court rejected. The journalistic exception applies to the processing of personal data that takes place exclusively for journalistic purposes, which the court ruled was not the case. The broadcasting of amateur football matches could not be regarded as a disclosure to the public of information, opinions or ideas. The matches broadcasted were not deemed to be sufficiently 'newsworthy' so as to fall within this exception, given the amateur nature of the sports and games. The reliance on the journalistic exception was therefore rejected. The platform also claimed that it had a legitimate interest – within the meaning of article 6(1)(f) GDPR - in processing the	23 November 2020	Court Ruling (in Dutch)

Development	Summary	Date	Links
	personal data concerned. The DDPA took the view that this was not the case, as a purely commercial interest can never be regarded as a legitimate interest. The Court found against the DDPA and gave extensive reasons for its judgment. The DDPA took the view that a legitimate interest is an interest that must be designated as a legal interest in (general) legislation or elsewhere in the law - the so-called "positive test". Moreover, the interest enshrined in legislation must be more or less urgent and specific in nature. Purely commercial interests and the interests of profit maximisation are not specific enough, and lack an urgent 'legal' character. Therefore, according to the DDPA, such interests cannot be regarded as legitimate interests. With reference to the case law of the Court of Justice of the European Union and an opinion of the Working Party 29 (the predecessor of the European Data Protection Board), the court considered that there is no clear definition of what constitutes a legitimate interest. There may be many interests at stake, whether trivial or compelling, whether obvious or controversial, with them being real and present - not just speculative. The court noted that, in practice, legal interests, as well as all kinds of factual, economic and idealistic interests, can qualify as legitimate interests. According to the court, a so-called 'negative test' must be applied: the controller may not pursue an interest that is contrary to the law (and therefore also not contrary to the statutory purpose of the controller). Once it has been established that the controller's interest qualifies as a legitimate interest (step 1), it still has to be assessed whether the processing is necessary to protect that legitimate interest (step 2). This assessment of necessity must be carried out in accordance with the requirements of proportionality and subsidiarity. Then - step 3 - a balancing of interests between the interests of the controller and the data subjects must be carried out, whereby the interests of the data subject must prevail. In this case, the DDPA had only examined in the investigation whether there was a legitimate interest (Step 1). Step 2 and step 3 had been skipped by the DDPA. It was only after the decision on the fine had been made that the DDPA reasoned that these requirements had not been met. The court eventually came to the		

Development	Summary	Date	Links
	conclusion that, because the investigatory report on the basis of which the fine decision was taken was incomplete, and therefore negligent, it should be annulled. The court then settled the case itself by making a new decision and cancelling the fine.		
The DDPA provides critical advice regarding the processing of biometric data regarding foreign nationals	The DDPA has commented on the proposed amendment of the Dutch Act on Biometrics in the Immigration Process ("**Wbvk**"). This Act enables, under certain circumstances, the collection and registration of biometric data of foreign nationals in order to combat identity fraud. The DDPA objected to the amended Act, stating that the current working method does not sufficiently protect the privacy of foreign nationals. The DDPA has advised the Minister for Migration not to continue with the legislative procedure unless the advice of the DDPA has been examined and their objections have been addressed.	6 November 2020	DDPA Statement (in Dutch)
The DDPA investigates data processing agreements in the private sector	The DDPA has investigated data processing agreements of 31 organisations in the private sector (from the trade, healthcare, media, leisure and energy sectors). The aim was to get a better picture of how such organisations draw up these agreements. The conclusion is that there is a wide variety of data processing agreements in use. The DDPA emphasised that periodically reviewing and updating data processing agreements are part of good business practice. Therefore, the DDPA has drafted a set of recommendations for organisations, including the following: – In your register of processing activities, specify the organisations that you engage; the categories of personal data that will be processed; the risks associated with this processing; and whether a data processing agreement is required. – Embed the drafting, assessment and the modification of data processing agreements in existing organisational procedures, for example by applying existing contract management procedures and by periodically reviewing the data processing agreements.	9 October 2020	DDPA Statement (in Dutch)

Development	Summary	Date	Links
	– Specify the measures and the agreements you have made. A processor agreement is meant to specify open standards from the GDPR for a specific situation. For example, it should specify retention periods and which security measures will be taken.		
The District Court Midden-Nederland held that files stored in OneDrive account are not necessarily personal data in the meaning of the GDPR	The claimant had purchased services from Microsoft, including the cloud storage service OneDrive. The agreement under which this service is purchased, namely the Services Agreement, was last renewed on 23 December 2019. At the beginning of April 2020, Microsoft denied the claimant access to his OneDrive account because of a serious breach of the code of conduct that forms part of the Terms of Service. Microsoft discovered child pornographic image in the OneDrive account of the plaintiff and blocked his account and his access to his files. The claimant is of the opinion that he has a right of access to the files on its OneDrive account on the basis of Article 15 (right of access) and Article 20 (right to data portability) of the GDPR. The claimant demanded to receive their files, with the exception of the image mentioned above, and sought the prohibition of the deletion of the other files in his OneDrive account. In a preliminary relief proceeding, the Court ruled that the child pornographic image constituted a violation of the Code of Conduct and ruled that, contrary to the claimant's contention, there was no question of an unreasonably onerous stipulation and that the sanction imposed by Microsoft was proportionate. Furthermore, the Court ruled that the files stored by the plaintiff were not automatically personal data within the meaning of Article 15 (right of access) and Article 20 (right to data portability) of the GDPR. The files did not contain information about the claimant. The fact that he had stored these files does relate to him personally, but does not make the files themselves personal data. The plaintiff also failed to provide any explanation as to how the files would constitute personal data within the meaning of the GDPR. Within the framework of these preliminary relief proceedings, the Court therefore concluded that the provisions of the GDPR did not oblige Microsoft to give the claimant access to the files stored by	8 October 2020	Court Ruling (in Dutch)

Development	Summary	Date	Links
	the claimant. However, the Court ruled that Microsoft is prohibited from deleting claimant's files, as it concerns a preliminary proceeding.		
The DDPA publishes revised recommendations for remote learning	The DDPA has investigated multiple educational institutions after receiving concerns and complaints from parents, students and teachers about the processing of personal data during remote learning. Based on recent investigations, the DDPA revised the previously published list of recommendations for remote learning, including (video) calling and online proctoring. For both online (video) calling and online proctoring, the DDPA considers it important that educational institutions set up institution-wide agreements or guidelines for the protection of privacy in order to avoid the need for each teacher to individually decide how they should deal with the personal data of the students. **Recommendations for online (video) calling** With online (video) calls, it is especially important that educational institutions draw up clear policies on the applications which may be used. This must specify what the video images may be used for. If it is not necessary, the educational institution must ensure that no students are in the picture when making video recordings of a digital lesson. The educational institutions must also ensure adequate agreements with the software supplier, including with regards to the retention period of the images. Images may not be kept longer than strictly necessary. **Recommendations for online proctoring** In online proctoring, educational institutions use software to supervise tests and exams that are made via the computer. A supervisor - or algorithm - then watches online to check whether a student is committing fraud. Online proctoring has a major impact on the privacy of students. That is why the educational institution has to meet strict requirements. For example, online proctoring may only be used if	2 October 2020	DDPA Recommendations (video calling, in Dutch) DDPA Recommendations (proctoring, in Dutch)

Development	Summary	Date	Links
	it is really necessary. This means that there are no alternative means by which the exam may go ahead. Furthermore, the invasion of privacy with online proctoring must be as limited as possible, and students must be informed about their privacy rights.		

Russian Federation

Contributors

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

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

Development	Summary	Date	Links
New penalties for Internet providers and owners of Internet platforms	A new bill on penalties for Internet providers and owners of Internet platforms for refusing to delete information prohibited in the Russian Federation at the request of the authorized Russian agency (Roskomnadzor), was adopted on 30 December 2020. The maximum fine for Internet providers and owners of Internet platforms prescribed in the bill is RUB 8,000,000. The penalty for companies who repeatedly refuse to remove such material is calculated based on their revenue. It could be up to 1/5 of the total amount of revenue for the calendar year preceding the year in which the administrative offense was identified. According to the preamble of the bill, fines cover Internet providers, and owners of Internet platforms, for any refusal to delete information prohibited in Russia, including social media platforms. Previously, there were no fines for refusal to delete prohibited information. The Law came into force on 10 January 2021.	30 December 2020	The official text of the bill and its stages
New ways of electronic communications with remote employees	A new bill regulating and defining remote work in Russia (and related nuances) was also adopted as a Federal Law dated 08 December 2020 No. 407-ФЗ. The bill provides for a wider application of electronic documents and e-signatures including electronic employment contracts. When concluding employment contracts and other contracts in electronic form, as well as when making changes to these	8 December 2020	The official text of the bill and its stages.

Development	Summary	Date	Links
	contracts and terminating them by exchanging electronic documents, the employer must use a qualified electronic signature, and the employee may use a qualified or an unqualified electronic signature according to the Russian Law "On electronic signatures". In other cases, the interaction between the remote employee and the employer can be carried out by exchanging electronic documents using other types of electronic signatures or in another form provided for by the company (for example, by describing it in the company policy). The Law came into force on 1 January 2021.		
New rules for processing publicly available personal data	A recently adopted bill changed and specified ways of processing publicly available personal data. In particular, the operator of personal data (similar to data controller status) must receive separate consent from the data subject for dissemination of data subject's personal data. Thus, consent is the main basis for making personal data publicly available and processes it as an operator of personal data. The authorized Russian agency (Roskomnadzor) must approve the content of such consent. Also, the data subject can include some restrictions regarding dissemination of data subject's data, for example, by restricting the transfer of personal data to third parties (however in the case third parties could have access to such personal data anyway, because they become publicly available). The silence or inaction of the data subject under no circumstances can be considered as consent for data dissemination. Furthermore, these changes provide a right for the data subject to send a request to pull their personal data from public access without additional conditions. The Law comes into force on 1 March 2021.	30 December 2020	The official text of the bill and its stages. The official publication on the Kremlin's website with the short summary

Russian Federation

Development	Summary	Date	Links
New grounds for access restrictions on the Internet	A recently adopted bill aimed at combating censorship by foreign Internet platforms in relation to Russian media materials was adopted on 25 December 2020. According to the law, the authorised Russian agency (Roskomnadzor) will be able to completely or partially block Internet resources that censor significant information in the territory of the Russian Federation on the grounds of nationality, language, origin, property and official status, profession, place of residence and work, attitude to religion and (or) in connection with the introduction of political or economic sanctions against Russia or Russians by foreign states. The Law came into force on 10 January 2021.	25 December 2020	The official text of the bill and its stages

Spain

Contributors

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

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

Development	Summary	Date	Links
The Spanish Data Protection Agency issues its Guide on Data Protection by Default	The Guide on Data Protection by Default (the "**Guide**"), issued by the Spanish Data Protection Agency ("**AEPD**"), develops the measures to be implemented to apply data protection by default. As stated by the European Data Protection Board in its "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", the implementation of these measures focuses on optimisation, configurability, and restriction strategies. – The aim of optimisation is to analyse processing from the point of view of data protection, which means applying measures in relation to the amount of personal data collected, the extent of the processing, the period of storage and the accessibility of personal data. – The configurability of applications, devices or systems must allow the setting of parameters or options that determine the way in which the processing is to be carried out, and must be capable of being modified by the data controller and by the user. – The restriction guarantees that, by default, the processing is as respectful of privacy as possible, so that the configuration options are adjusted, by default, to those settings that limit the amount of data collected, the extension of the processing, its conservation and accessibility.	8 October 2020	Guide on Data Protection by Default (in Spanish)

Development	Summary	Date	Links
	A document was also issued with a non-exhaustive list of measures and configuration parameters or options to implement the data protection by default strategies. Furthermore, the Guide includes a section on documentation and auditing requirements, aspects that are necessary to demonstrate compliance with the regulation (as established by the principle of accountability).		
The AEPD issues a tool to help data controllers decide whether to communicate a personal data breach to the data subject	The AEPD has issued "Comunica-Brecha RGPD", a tool which aims to promote transparency and accountability among data controllers when faced with the obligation to communicate a personal data breach to those affected. The tool is free of charge, easy to use and based on a short form that collects information to assess basic criteria that can be indicative of the risk associated with a personal data breach. The AEPD does not store the data submitted during the process. When the form is completed, and depending on the information provided, the tool offers three possible scenarios: – that data subjects must be notified of the personal data breach as a high risk is identified; – that such notification is not necessary; or – that the level of risk cannot be determined. The use of this tool does not in any case replace the necessary assessment of the level of risk by the data controller, who has the best knowledge of the details of the processing of personal data carried out, the characteristics of the data subjects, the circumstances of the personal data breach and the rest of the elements that make it possible to obtain an accurate assessment of the risk. Similarly, the use of said tool is independent of the obligation to notify such breaches to the supervisory authority.	22 October 2020	Tool "Comunica-Brecha RGPD" (in Spanish)
The AEPD approves the first Code of Conduct under the GDPR, the "Code of Conduct for the Processing of Data in Advertising Practice"	The AEPD, in the exercise of the tasks and powers attributed by the GDPR and the Spanish Organic Law 3/2018 of December 5, on the Personal Data Protection and Guarantee of Digital Rights ("**LOPDGDD**"), has approved the first code of conduct and accredited its monitoring body in accordance with the provisions of Articles 40 and 41 of the GDPR and 38 of the LOPDGDD.	3 November 2020	Code of Conduct for the Processing of Data in Advertising Practice (in Spanish)

Development	Summary	Date	Links
	The "Code of Conduct for the Processing of Data in Advertising Practice" ("**Code**") has been prepared by AUTOCONTROL, the independent advertising self-regulatory organisation (SRO) in Spain, which focuses mainly on: – the regulation of measures to demonstrate accountability in the processing of data for advertising purposes; and – the establishment of an extra-judicial system for resolving disputes between the entities adhering to the Code and the data subjects. The Code will only be applied to processing carried out by adhering entities located in Spain or that affect data subjects resident in Spain, provided that the processing refers to the offer of goods and services in Spain or to the control of their behaviour in said territory. As regards who should/must adhere to the Code, the entities included in the Code itself are: – the advertisers, agencies and media associated with AUTOCONTROL; – the associations or representative entities of a sector associated with AUTOCONTROL, on its behalf or on that of its representatives; and – any other entities of the advertising industry. Furthermore, on the occasion of the approval of the Code, the Register of Codes of Conduct has been implemented to publicise it, in accordance with Article 40(6) of the GDPR and Article 38.5 of the LOPDGDD.		

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: updated guidelines for processing by employers	The Swedish Authority for Privacy Protection (the "**Swedish DPA**") issued updated information on processing of personal data by employers. Among other things, the information clarifies the following points: – That consent is usually not a feasible legal basis in relation to employees, since it is typically not considered to be provided voluntary; and – That the employer should decide how employees may use its IT systems, and that the employer may under certain circumstances control such use. It is noted that, for example, logging of use of IT systems is often considered to be highly intrusive on an employee's privacy and must only be used in such way that it does not unduly interfere on the employee's privacy.	5 October 2020	Press Statement (In Swedish) Information site (In Swedish)
Swedish DPA: new guidelines to strengthen the protection of children	The Swedish DPA, together with the Ombudsman for Children and the Swedish Media Counsel, have issued guidelines to strengthen the protection and rights of children and young people online. The guidelines are largely aimed at companies that create or provide digital services widely used by children and they aim to make the internet a safer place for children. These guidelines are part of the measures based on that the UN Convention on the Rights of the Child, which become national law in Sweden during 2020. The guidelines include advice both from a privacy perspective and a children's rights perspective.	12 October 2020	Press Statement (In Swedish) Guidelines (In Swedish)

Sweden

Development	Summary	Date	Links
Swedish DPA: audit of an organisation is closed	Earlier in 2020, the Swedish DPA initiated an audit of a company based on a complaint received in relation to the company's processing of personal data on candidates in a recruitment process. The Swedish DPA concluded that the processing of personal data performed fell outside of the scope of the GDPR and consequently, closed the audit without further actions.	13 October 2020	Press Statement (In Swedish)
Swedish DPA issues a report on complaints received from data subjects	The Swedish DPA has issued a report based on the complaints received from data subjects since the GDPR entered into force. Since May 2018, the Swedish DPA has received around 3,000 complaints each year in relation to processing of personal data. Before the GDPR entered into force, this number was significantly lower, with around 500 complaints being recieved per year. The increased number of complaints clearly indicates a greater public awareness of and interest in the lawful processing personal data. The report is based on an analysis of 250 complaints. Out of these complaints, 25% relate to data subject's rights and the most common complaint is that data has not been erased despite the data subject request. The second most common complaint is that a record of data has not been provided despite the data subject requesting a copy. Additionally, the report shows that more than a tenth of the complaints relate to the data subjects concern that personal data is not being adequately protected.	20 October 2020	Press Statement (In Swedish) Report (In Swedish)
Swedish DPA initiates a number of audits based on complaints from data subjects	The Swedish DPA has received a numerous complaints from data subjects regarding their rights under the GDPR, which have led to a number of audits being initiated. These audits have a limited scope and will mainly focus on the subject matter of the complaint.	2 November 2020	Press Statement (In Swedish)
Swedish DPA imposes a fine of SEK 4,000,000 on the Board of Education in the City of Stockholm	The Swedish DPA has received a number of personal data breach notifications from the Board of Education in the City of Stockholm. All incidents relate to the school platform, which is an IT system used, among other things, for student administration. The IT system holds information on 500,000 pupils, guardians and teachers, including sensitive personal data. In reviewing parts of the IT system, the Swedish DPA found serious	24 November 2020	Press Statement DPA Decision (In Swedish)

Development	Summary	Date	Links
	shortcomings, including deficiencies in relation to user restrictions. For example, a large number of teachers could access information on pupils with a protected identity, and guardians where able to access information relating to other children. The Swedish DPA concluded that the deficiencies were serious, and that the Board of Education had failed to take adequate security measures to protect the personal data it processes. It should be noted that, in Sweden, the maximum amount of such fines against public authorities is SEK 10,000,000.		
Swedish DPA imposes a fine of SEK 200,000 on Gnosjö Municipality	The Swedish DPA received a complaint from a relative of a person residing at 'LSS housing', a residential care home for people with certain functional impairments. The relative claimed that the resident was being monitored illegally. The Swedish DPA initiated an audit, and did indeed conclude that the resident was monitored in their bedroom, in violation of the GDPR. The Social Welfare Committee in Gnosjö, responsible for the LSS housing, has stated that certain of needs of the residents, as a result of their conditions, led to the conclusion that the measures were necessary for the security of both the resident and for the staff. The Swedish DPA concluded that, although the measures were indeed necessary, there were more proportionate measures available which should have been put in place. It further highlighted that there was no legal basis for the monitoring, no data protection impact assessment had been performed, and the controller failed to inform the data subject that such monitoring was taking place. For these reasons, the DPA imposed a fine of SEK 200,000 on the Social Welfare Committee.	25 November 2020	Press Statement DPA Decision (In Swedish)
Swedish DPA initiates audits of transfers to third countries	The Swedish DPA has initiated 6 audits based on complaints received from the organisation None of Your Business ("**NOYB**") regarding transfers of data to third countries. These audits were conducted as part of the working group established by the European Data Protection Board (EDPB) to handle a large number of complaints received from NOYB across the EU.	26 November 2020	Press Statement (In Swedish)

Sweden

Development	Summary	Date	Links
Swedish DPA imposes fines of up to SEK 30,000,000	The Swedish DPA has finalised audits of 8 health care providers. The primary focus of the audits was whether the health care providers had performed a needs and risk analysis required in order to assign an adequate access authorisation for personal data in the electronic health records. The Swedish DPA noted that 7 out of the 8 health care providers audited had not performed such analysis. While the 8th provider had performed the required analysis, the analysis carried out included some shortcomings. This meant that 7 out of the 8 health care providers had not taken appropriate measures to ensure and be able to demonstrate an adequate level of security for the personal data they process. These are serious deficiencies, and as a result the DPA has imposed fines of between SEK 2,500,000 and SEK 30,000,000 on the providers. The level of the fine varies greatly, partly based on whether the health care provider is a private company or a public authority. For public authorities, the maximum fine is SEK 10,000,000.	3 December 2020	Press Statement Swedish Press Statement with links to all decisions (In Swedish)
Swedish DPA imposes a fine of SEK 550,000 on Umeå University	The Swedish DPA performed an audit of Umeå University based on its processing of sensitive personal data without sufficient protection. A research group at Umeå University had requested information from the Swedish Police on preliminary investigation reports concerning cases of male rapes. The reports included sensitive personal data such as suspicion of crime and sexual life and health. The research group scanned these reports into an American cloud service. The manner in which the University used the cloud service did not provide sufficient protection to the personal data processed. Furthermore, the research group communicated sensitive personal data via unencrypted email, despite the Police pointing out the inappropriateness of doing so. The University also failed to notify the Swedish DPA of this data breach. Based on the infringements it had identified, the Swedish DPA imposed a fine of SEK 550,000 on the University.	11 December 2020	Press Statement DPA Decision (In Swedish)

Sweden

Development	Summary	Date	Links
Swedish DPA imposes a fine of SEK 300,000 on housing company	The Swedish DPA initiated an audit of a housing company following receipt of a complaint claiming that a surveillance camera was directed towards the complainant's front door. The housing company states that the purpose of the video surveillance was to resolve disturbances in the stairwell over time. The video surveillance covered the front doors of two apartments in particular; one of these belonged to the complainant, and the other to a resident who had been subject to disturbances and harassment. It was found that even if the housing company had a legitimate interest to carry out the video surveillance, this was outweighed by the resident's right to privacy. The DPA imposed a fine of SEK 300,000 on the housing company, and the housing company has since ceased its video surveillance.	15 December 2020	Press Statement DPA Decision (In Swedish)
Swedish DPA initiates audit of SIS-II	The Swedish DPA has initiated an audit of the Swedish part of the Schengen Information System, SIS-II. Such audit is to be performed by all EU-countries every fourth year.	16 December 2020	Press Statement (In Swedish)
Swedish DPA finalises audits of law enforcement agencies	The Swedish DPA has performed an audit of seven law enforcement agencies. The audits were focused on the agencies' ability to discover data incidents and manage and document potential incidents. They also looked at the information and training staff had been provided in relation to data incidents. The Swedish DPA concluded that the procedures of the agencies in relation to data incidents were good, and closed the audits by providing a number of recommendations to the agencies. The recommendations included the performance of an annual review of the measures in place to discover incidents, to continuously control whether the routines are followed and to continuously inform staff on how incidents should be handled.	18 December 2020	Press Statement (In Swedish)

Switzerland

Contributors

Markus Näf
Partner
T: 41 44 204 90 90
markus.naef@
eversheds-sutherland.ch

Michel Verde
Senior Associate, Attorney-at-Law
T: +41 44 204 90 90
michel.verde@
eversheds-sutherland.ch

Development	Summary	Date	Links
Swiss Federal Tribunal concretises the data subject's access right	The Swiss Federal Tribunal, which is the highest court in Switzerland, recently had the opportunity to address two cases regarding the boundaries of the data subject's access right under the Swiss data protection law. According to article 8 of the Swiss Federal Act on Data Protection, a data subject has the right to obtain information from the controller as to whether their personal data is being processed. This includes, in particular, detail on all personal data concerning the data subject, which is contained in a data file, the source of the data, the purpose of and (if necessary) the legal basis for the processing, as well as the categories of personal data processed relating to other parties involved and the data recipients. In the first case (4A_277/2020 of 18 November 2020), the Federal Tribunal had to deal with the question of the point at which a data subject access request would be deemed abusive, and can therefore be rejected. The Federal Tribunal emphasised that the purpose of the access right is to enable the data subject to check whether the personal data processed about him/her in a data file is processed in accordance with the principles of Swiss data protection law, and to enforce compliance with these principles. In contrast, an access request will be considered abusive if it is made for purposes other than the realisation of the purpose for which this right has been created. According to the Federal Tribunal, this would be the case where, for example, the access right is exercised: (i) to save the costs for obtaining data that would otherwise have to be paid, (ii) to hassle the controller, or (iii) to obtain evidence that the data subject could not obtain otherwise. In the case at hand, the Federal Tribunal concluded that the only purpose of the data subject's access request was to	Date of 1st Decision: 18 December 2020 Date of 2nd Decision: 10 December 2020	

Development	Summary	Date	Links
	assess the prospects of success of an intended litigation, and therefore considered the access request to be abusive. This was the first time that the Federal Tribunal had considered a data subject's access request to be abusive, because the threshold to classify such request as abusive is very high. In the second case (4A_125/2020 of 10 December 2020), the Federal Tribunal had to deal with the question of whether a data subject's access right also includes personal data that is not physically available, but 'kept in mind' by the controller. The data subject requested access to personal data that the controller supposedly received from a third party in the course of a conversation. Since there was no note or other record of that conversation, the Federal Tribunal had to decide whether the access right also encompasses personal data that is only available in the controller's memory. The Federal Tribunal concluded that a data subject's access right is limited to personal data that is available in writing or another physical form, and can therefore be objectively accessed. There is no right for such requests to include personal data that can only be retrieved from memory.		

United Kingdom

Contributors

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

Erica Werneman Root
Senior Associate
T: +44 20 7919 4860
ericawernemanroot@
eversheds-sutherland.com

Development	Summary	Date	Links
ICO opens consultation on draft statutory guidance on the ICO's powers and how fines are calculated	The ICO has opened a public consultation on its draft Statutory guidance, in line with the DPA 2018. The draft guidance highlights the ICO's role in regulating and enforcing UK data protection legislation; it details the ICO's powers and how fines are calculated. The ICO has stressed that its primary function is to protect the rights and freedoms of individuals. The consultation closed at 5pm on 12 November 2020.	1 October 2020	Press release Draft guidance Consultation
New guidance released on Gov.UK relating to data protection and data flows: preparing businesses for the end of the transition period	The Department for Digital, Culture, Media & Sport ("**DCMS**"), the Department for Business, Energy & Industrial Strategy ("**BEIS**"), the Office for Civil Society ("**OCS**") and Information Commissioner's Office ("**ICO**") have produced and published updated guidance titled "using personal data in your business or other organisation after the transition period". This aims to assist businesses in preparing for the end of the transition period by setting out steps they need to take regarding data protection and data flows within the EU/EEA following 31 December 2020.	2 October 2020	Updated Guidance
Committee publishes correspondence on UK government's view of Schrems II and adequacy decisions	The European Scrutiny Committee (the "Committee") has published correspondence with the Minister of State for Media and Data. The Committee has requested the government's view on the Schrems II decision, and the UK's plans for data adequacy decisions after Brexit. The Committee wrote in response to the Minister's letter of 18 September.	6 October 2020	Letter
UK Information Commissioner Elizabeth Denham addresses PDP's	The Information Commissioner presented the keynote speech at a data protection conference held on 8 October 2020.	8 October 2020	Speech

Development	Summary	Date	Links
19th annual data protection conference	In her speech the Commissioner emphasised the need for transparency with individuals which has only been furthered in the pandemic, and the need for organisations to take on more accountability for their role in collecting, using and transferring personal data. In particular, the Commissioner highlighted key themes for the coming year, particularly in balancing the needs of "liberty, privacy innovation and prosperity" and how we can ensure that there is continued innovation whilst at the same time protecting individuals' freedoms; this being helped by increasing need for international collaboration and cooperation with other regulatory bodies. One element which the Commissioner was keen to address was the role of the ICO with Brexit and legislative changes. In particular she stated the ICO is not there to "make or shape laws" but instead to assist in navigating what government and parliament agree.		
Information Commissioner publishes blogpost highlighting ICO work during COVID-19 pandemic	Information Commissioner has published a blog post which looks at the ICO's work during the Coronavirus pandemic. The piece points to the ICO's work to help bodies with the shielding and manual contact tracing, how to properly gather and process details and the carrying out of Data Protection Impact Assessments in England and Wales, Northern Ireland and Scotland. Denham noted that what is important in every piece of technology or service being developed to tackle the virus is that people's privacy rights are being considered at the heart of those apps and services.	13 October 2020	Blogpost
UK government response to Report on misinformation amid COVID-19	In July 2020, the Digital, Culture, Media and Sport Committee published a report titled 'Misinformation in the Covid-19 Infodemic' (the "**Report**"). The Government's response to the Report has now been published, which stressed the importance of accurate information reaching the public during this time of emergency, and recognised the disinformation and misinformation circulating online about Covid-19.	14 October 2020	Report Government response

Development	Summary	Date	Links
	The Government aims to publish the Online Harms full Government Response by the end of 2020; the full Response will include full responses to all of the Report's recommendations. The full Response will detail policy proposals, and will be followed by legislation in early 2021.		
£18.4m fine for Marriott, following a cyber attack which commenced in 2014	The ICO has announced another significant fine for a personal data breach. Marriott International Inc. has been fined £18.4m for a cyber attack at one of Marriott's subsidiaries which commenced in 2014 (indeed, before Marriott acquired the subsidiary). Marriot acquired the subsidiary in 2016 (at which point the cyber attack was still ongoing) but it was not until September 2018 (after GDPR was in force) that Marriot finally identified that the subsidiary's IT systems were currently compromised, at which stage the ICO was notified. It was estimated that 339 million guest records were affected by the cyber attack, albeit that a portion of the information affected was encrypted. The fine of £18.4m was notwithstanding that the ICO had not seen any evidence of financial harm to individuals. This case demonstrates the importance of due diligence in acquisitions (and indeed post-acquisition audits, and regular audits generally). Had the cyber attack been identified and resolved prior to 25 May 2018 (when GDPR came into force), the ICO would only have been able to impose a fine of up to £500,000 (which was the cap for fines under the Data Protection Act 1998 which preceded GDPR), significantly less than the £18.4m fine imposed here.	30 October 2020	Press release Penalty notice (pdf)
DCMS updated guidance on data protection and data flows post-Brexit transition	The Departments for Digital, Culture, Media & Sport, Business, Energy & Industrial Strategy ("**DCMS**"), Office for Civil Society and the ICO have published updated (high-level) guidance on data protection at the end of the post-Brexit transition period (and beyond). Notably, the guidance states that the Government is '*confident*' that an EU adequacy decision in respect of the UK can be concluded by the end of the transition period (however, it points out that if an adequacy decision is not concluded, UK entities will need to act to ensure they can continue to lawfully receive personal data from EU entities). For background, after the end of the transition period, transfers from EU entities to UK entities will constitute a transfer by the EU entity to a third party outside of the EEA, triggering a requirement that the transfer is	16 November 2020	Guidance

Development	Summary	Date	Links
	made pursuant to one of the approved transfer mechanisms set out in the GDPR (one of which would be an adequacy decision, if one is concluded, which would negate the need to enter into eg SCCs (see updates above for more details about SCCs and alternative transfer mechanisms for exporting personal data outside of the EEA)). The guidance also reaffirms the UK's previously stated position that no such transfer mechanism will be required for transfers from the UK to the EEA (or countries who currently have an adequacy decision from the EU), but states that if this changes the guidance will be updated.		
Detailed guidance on processing criminal offence data issued by ICO	The ICO has updated its guidance on the processing of criminal offence data, including issuing some new detailed guidance. The new detailed guidance is an important resource for UK entities who process criminal offence data. Amongst other things, it clarifies that the concept of criminal convictions covers information relating to the *absence* of such convictions (ie a 'clear' criminal record check still constitutes processing of criminal offence data), and furthermore that details about victims will also be caught within this concept. Additionally, notwithstanding that civil proceedings/orders will not generally be caught, they will be caught if the penalty for non-compliance with the order comes with a criminal sanction (eg restraining orders).	6 November 2020	General guidance (updated) Detailed guidance (new)
Brexit trade agreement and transfers of data from the EU to the UK, with ICO and CNIL (French DP regulator's) statements.	After the signing of the Brexit deal on 31 December, the UK Government announced that the Treaty which had been agreed with the EU allows for the free flow of personal data from the EU and EEA to the UK. This is a temporary measure which will last for no more than 6 months and will only be in place until adequacy decisions have been reached. Additionally, the UK has, on a transitional basis, deemed the EU and EEA EFTA States to be adequate to allow for data flows from the UK. The extension is welcome news and will enable businesses and public bodies across all sectors to continue to freely receive personal data from the EU (and EEA). This includes data from law enforcement agencies, which will be critical for business and security within the UK. The ICO have made a recommendation that businesses who rely on personal data transfers should engage with the EU and EEA	28 December 2020	ICO statement

Development	Summary	Date	Links
	entities who transfer data to them to establish alternative mechanisms. This should offer protection to business should the free flow of data be cut short. Ireland's Data Protection Commission echoed the statements above in its guidance on 5 January 2021 and noted that Irish-based data exporters can continue to transfer the personal data to UK-based data importers in 2021 during the 6 month temporary measures without the need for mechanism such as Standard Contractual Clauses. Additionally on 4 January the German Data Protection Conference issued guidance on the same.		

United States

Contributors

Michael Bahar
Partner
T: +1 202 383 0882
michaelbahar@
eversheds-sutherland.com

Mary Jane Wilson-Bilik
Partner
T: +1 202 383 0660
mjwilson-bilik@
eversheds-sutherland.com

Sarah Paul
Partner
T: +1 212 301 6587
sarahpaul@
eversheds-sutherland.com

Alexander Sand
Associate
T: +1 512 721 2721
alexandersand@
eversheds-sutherland.com

Margaret Flatt O'Brien
Associate
T: +1 404 853 8070
margaretobrien@
eversheds-sutherland.com

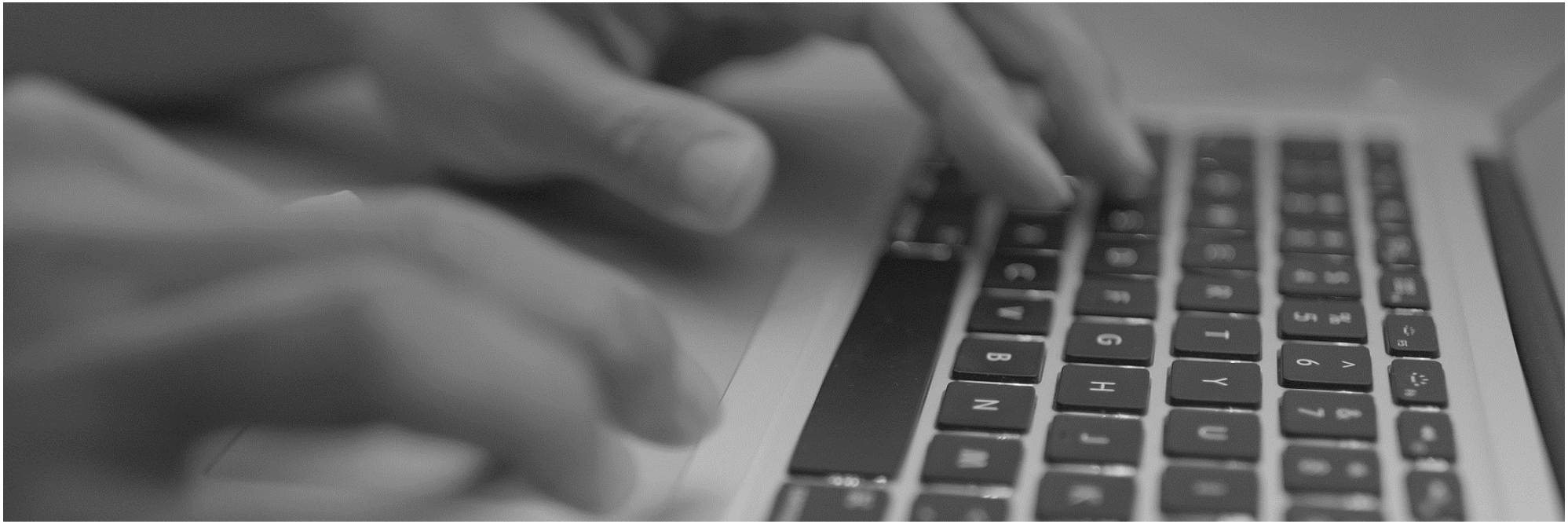
Development	Summary	Date	Links
The US Department of the Treasury issued an advisory warning that ransomware payments may violate OFAC regulations, resulting in sanctions	On 1 October 2020, the US Department of the Treasury's Office of Foreign Assets Control ("**OFAC**") issued an advisory alerting companies that facilitating ransomware payments could lead to potential sanctions violations. The advisory states that ransomware victims who pay ransom amounts and third-party companies that negotiate or pay ransom on their behalf encourage future attacks and risk violating OFAC regulations. More specifically, a ransomware payment might include a person or jurisdiction on the OFAC sanctions list. As a result, the advisory encourages ransomware victims and third parties involved in addressing attacks to contact OFAC if they believe a request for payment would implicate sanctions.	1 October 2020	OFAC Advisory

Development	Summary	Date	Links
The US Department of Justice issued Cryptocurrency Enforcement Framework	On 8 October 2020, the US Department of Justice ("**DOJ**") Cyber-Digital Task Force issued an 83-page comprehensive "Cryptocurrency: An Enforcement Framework," (Framework), signaling the DOJ's increased focus on prosecuting crimes involving cryptocurrency. The Framework provides insight into DOJ's perspective and policies on cryptocurrency enforcement and addresses: (1) the threats posed by cryptocurrency, (2) available cryptocurrency enforcement tools, and (3) the challenges of cryptocurrency enforcement. First, the Framework describes three categories of activities involving the potential illicit use of cryptocurrency: "(1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements, [and] (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself." The Framework then outlines both criminal and civil legal and regulatory tools that the US government may use to confront illegal cryptocurrency use. The Framework concludes with a discussion of enforcement challenges unique to cryptocurrency cases.	8 October 2020	Cryptocurrency Enforcement Framework
California's new privacy law, the California Consumer Privacy Act, was approved, imposing increased privacy obligations on businesses that process California consumers' personal information	On 3 November 2020, California voters passed Proposition 24, the California Privacy Rights Act (the "**CPRA**"). Once it goes into effect on 1 January 2023, the CPRA will amend and supersede the California Consumer Privacy Act (the "**CCPA**"). The CPRA builds on the existing framework of the CCPA, expands consumer privacy rights to more closely align with the EU's GDPR, imposes additional obligations on businesses, and establishes the nation's first agency dedicated to privacy regulation and enforcement, the California Privacy Protection Agency (the "**CPPA**"). The law's passage will have some immediate impacts, including: – Exemptions for employee and business-to-business data are extended until 1 January 2023. – The watchdog privacy agency, the CPPA, becomes effective immediately. The CPPA's five-member board must be appointed within 90 days of the law's enactment, which	3 November 2020	California Privacy Rights Act

Development	Summary	Date	Links
	occurs 5 days after the Secretary of State certifies the final vote. Other key provisions include: a new sub-category of "sensitive" personal information, a new definition of "third party," a new definition of "profiling," limits on data retention and required disclosure of retention periods, a right to limit use and disclosure of sensitive personal information, a right to correct inaccurate personal information, an extension of consumer opt-out rights, an extension of the non-discrimination provision, additional contact requirements for all persons that receive personal information, increased administrative fines for children's personal information, required opt-in consent for sharing personal information of children under 16, establishment of the CPPA, requirement for new rulemaking on cybersecurity and privacy, and an extension of the scope of the private right of action.		
The Seventh Circuit clarified standing in federal court for Illinois Biometric Privacy Act claimants	On 17 November 2020, the Seventh Circuit held in *Fox v. Dakkota Integrated Systems* that an Illinois plaintiff that asserted a violation of Section 15(a) of the Illinois Biometric Privacy Act (BIPA) had sufficient standing to sue in federal court.	17 November 2020	Fox v. Dakkota Integrated Systems
The Supreme Court is examining whether it is a federal crime under the Computer Fraud and Abuse Act to use one's authorized access to a computer for inappropriate purposes	On 30 November 2020, the Supreme Court heard arguments in *Van Buren v. U.S.,* in an effort to resolve a circuit split among appeals courts that have reached different conclusions on whether employees, or anyone else authorized to access a computer, face criminal or civil liability for abusing that authorization to access information for improper purposes under the Computer Fraud and Abuse Act (the "**CFAA**"). Last amended in 2008, the CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization, but fails to sufficiently define "without authorization" and "exceed authorized access." 18 U.S.C. § 1030(a)(2). This language has created a circuit split. It is possible that the Supreme Court can find a narrow way to rule, in part to incentivize Congress to resolve the issue. On the other hand, a Supreme Court endorsement of the broader interpretation could mean that even violating website terms of use and company policies can be read to "exceed authorized	30 November 2020	Van Buren Oral Arguments

Development	Summary	Date	Links
	access," effectively enabling companies to issue policies that turn conduct into a federal crime.		
The President signed the first-ever federal law governing Internet of Things devices	On 4 December 2020, then President Donald Trump signed the first-ever federal law governing Internet of Things (**IoT**) devices. The IoT Cybersecurity Improvement Act (the "**Act**") will result in new national rules for federal procurement of IoT devices. The Act builds upon and helps to unify the varying cybersecurity standards within federal procurement regulations, including the Defense Federal Acquisition Regulation Supplement (FAR), in order to better secure government networks, infrastructure and systems.	4 December 2020	IoT Cybersecurity Improvement Act
The New York Department of Financial Services required all New York financial institutions to report effects of the SolarWinds security breach	The massive SolarWinds security breach, dating back to perhaps March of 2020, affected not only the private sector, but also federal, state and local governments. On 18 December 2020, the New York Department of Financial Services ("**NY DFS**") made it very clear that regulated entities—including banks, insurance companies, and financial advisors—must share information related to the hack, even when the normal reporting standard under the NY DFS Cybersecurity Regulation has not been met.	18 December 2020	NY DFS Issued Industry Guidance
The Financial Crimes Enforcement Network proposed new recordkeeping, verification, and reporting requirements for transactions involving virtual currency and digital assets	On 18 December 2020, the Financial Crimes Enforcement Network ("**FinCEN**") issued a Notice of Proposed Rulemaking ("**NPRM**") to establish new requirements for convertible virtual currency ("**CVC**") and legal tender digital asset ("**LTDA**") transactions. The NPRM is a response to the rise in illicit financial threats posed by alleged bad actors taking advantage of the anonymity offered by CVC and LTDA transactions. The proposed rule, which would affect US banks and money services businesses ("**MSBs**"), would expand existing reporting, verification and recordkeeping obligations under the Bank Secrecy Act ("**BSA**") to CVC and LTDA transactions, add a new prohibition on "structuring" to avoid reporting obligations, and expand the definition of "monetary instrument" to include CVC and LTDA transactions. FinCEN has also proposed two exemptions to the reporting requirement: (1) transactions between hosted wallets held at	18 December 2020	FinCEN NPRM

Development	Summary	Date	Links
	financial institutions subject to the BSA; and (2) CVC or LTDA transactions where a foreign financial institution hosts the counterparty wallet, unless that institution is located in a jurisdiction on the new "Foreign Jurisdictions List," which FinCEN will establish and maintain.		
New York temporarily banned the use of facial recognition technology in schools	On 22 December 2020, New York Governor signed into law legislation that temporarily bans the use or purchase of facial recognition and other biometric identifying technology in schools until at least 1 July 2022. The legislation also directs the New York Commissioner of Education to conduct a study on whether this technology is even appropriate for use in schools.	22 December 2020	Governor's Office Press Release



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

Erica Wernemann Root
Senior Associate
T: +44 20 7919 4860
ericawernemanroot@eversheds-sutherland.com

Rosie Wallace
Apprentice Solicitor
T: +44 20 7919 4942
rosiewallace@eversheds-sutherland.com

Lucy Clarkson
Apprentice Solicitor
T: +44 113 200 4536
lucyclarkson@eversheds-sutherland.com

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

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

eversheds-sutherland.com

CAM_1B\7255141\7