EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

April to June 2021
Edition 12

Executive summary

Welcome to the latest edition of Updata!

Updata is an international report produced by Eversheds Sutherland's dedicated Privacy and Cybersecurity team – it provides you with a compilation of key privacy and cybersecurity regulatory and legal developments from the past quarter.

This edition covers **April to June 2021** and is full of newsworthy items from our team members around the globe, including:

- the European Commission's publication of new standard contractual clauses for international data transfers and for contracts between controllers and processors;
- guidelines from the EDPB on the targeting of social media users;
- final recommendations from the EDPB on supplementary measures for data transfers;
- new Austrian case law concerning data retention, parliamentary investigations and the exchange of taxation data;
- the publication of the second draft of China's Personal Data Protection Law, as well as the passing of China's new Data Security Law;
- the Dutch data protection authority issuing a fine for failure to appoint an EU representative pursuant to the GDPR;
- proposed legislation in Russia including in relation to the conversion of paper documents into electronic format, the expansion of information monitored by social media networks and the requirement for tech companies to open offices in Russia;
- new guidance from the Spanish data protection authority in relation to data protection and labour relations, breach notifications and data protection impact assessments; and
- the adoption of EU adequacy decisions in respect of the UK to enable the free flow of personal data from the EEA to the UK.

We hope you enjoy this edition of Updata.

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

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

Follow us on Twitter at:
@ESPrivacyLaw

General EU and International

Contributors

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

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

Development	Summary	Date	Links
EDPS publishes Annual Report 2020	The European Data Protection Supervisor ("**EDPS**") published its Annual Report 2020. The report focuses on the ways in which the EDPS maintained its role as the data protection authority for EU institutions throughout the COVID-19 pandemic. Themes include: – the establishment of an internal COVID-19 taskforce to coordinate and carry out work surrounding the impact of the pandemic on data privacy; – EDPS advocating a pan-European approach to fighting the virus with a particular emphasis on contact tracing apps; the maintenance of a strong level of oversight over the EU Institutions, Agencies and Bodies' processing of individuals' personal data; – the introduction of online audits; issuing more Opinions and Comments to the European Commission, the European Parliament and Council than ever before; – the creation of open source software tools in the context of automating privacy and personal data protection inspections of websites; and – proposing the creation of the Support Pool of Experts to help strengthen the enforcement of data protection law in the EU. The report also highlights the EDPS's commitment to making sure that EU institutions comply with the *Schrems II* judgment through the publication of a strategic document.	20 April 2021	Press release Summary Report Strategy (compliance with Schrems II judgment) Strategy (EDPS Strategy 2020 – 2024)

Development	Summary	Date	Links
	Finally, the report launched the new EDPS Strategy for 2020 to 2024. The new Strategy will seek to shape a safer digital future and will focus on three pillars: Foresight, Action and Solidarity.		
European Commission publishes proposals for new legal frameworks on Artificial Intelligence and Machinery	The European Commission published its proposals for a new legal framework on AI ("**Proposed AI Regulation**"), a coordinated plan regarding AI with Member States, and a new regulation on Machinery ("**Machinery Regulation**"). Read our full client briefing on the Proposed AI Regulation here. Following a risk-based approach, the Proposed AI Regulation will split the rules governing AI into categories: – Unacceptable risk – AI systems in this category will be banned (e.g. 'social scoring' systems). – High-risk – including, for example, remote biometric identification systems. These AI systems will be subject to rigorous obligations including risk assessments and mitigation systems. – Limited risk – e.g. chatbots. Transparency obligations that are specific to the system will be necessary e.g. for chatbots, a reminder to users that they are talking with a machine. – Minimal risk – most AI systems fall under this header. the Proposed AI Regulation does not cover systems that are classed as minimal risk . The establishment of an European Artificial Intelligence Board is also proposed, which will govern the application and implementation of the new rules surrounding AI. In addition, several voluntary codes of conduct regarding non-high-risk AI are planned for publication. Regulatory sandboxes will also be established in order to enable responsible innovation. A new coordinated plan will build on the current coordinated plan that was published in 2018. The new plan will focus on the following goals: – the creation of enabling conditions for the development of AI through investment and knowledge sharing;	21 April 2021	Press release Eversheds Sutherland client briefing Proposed regulation (AI) Plan Proposed regulation (Machinery)

Development	Summary	Date	Links
	– fostering AI excellence through creating research, development and innovation opportunities and facilities; – ensuring that AI is a force for good in society through enabling the development and deployment of 'trustworthy' AI; and – strengthening strategic leadership in the AI context within high-impact sectors and technologies e.g. environment. It is proposed that the current Machinery Directive will be replaced by the new Machinery Regulation. The Machinery Regulation will seek to protect the safety of machine users, encourage innovation, ensure the safe integration of AI into machinery and will provide greater legal clarity on the current provisions. The European Parliament and the Member States will move towards adopting the Commission's proposals on the Proposed AI Regulation and the Machinery Regulation. At the same time, the Commission will work with Member States to put the actions detailed in the Coordinated Plan into action.		
EDPS publishes statement on Proposed AI Regulation	The EDPS published a statement welcoming the Proposed AI Regulation (see above), and expressing approval of its new role as the AI regulator for the EU public administration. The EDPS is critical of the European Commission's failure to use the Proposed AI Regulation to address the use of remote biometric identification systems in public spaces. The EDPS calls for a stricter approach to regulating these systems, owing to their potential to intrude deeply into individuals' private lives. The EDPS will now commence analysing the Commission's proposal in detail.	23 April 2021	Press release
EDPB finalises guidelines on the targeting of social media users	The European Data Protection Board ("**EDPB**") published Guidelines 8/2020 on the targeting of social media users. The guidelines will be useful for organisations engaging with social media as part of their marketing initiatives. The guidelines focus on the collection and use of personal data through targeting services offered by social media platforms. The	23 April 2021	Guidelines

Development	Summary	Date	Links
	services involve sharing data on an individual's personal characteristics. This information is either collected with the consent of the individual, or observed / inferred by the platform or by third parties and aggregated with other data to build up a picture of an individual. The resulting profile is used in order to target users with messages that 'fit' their profile. This process is called "targeting". The EDPB considers the "combination and analysis of data originating from different sources, together with the potentially sensitive nature of personal data processed in the context of social media" creates risks to individuals' fundamental rights and freedoms, including scope for infringing data protection rights as well as discrimination, exclusion and user manipulation. The guidelines explores the data protection roles and responsibilities at play in various social media targeting scenarios (including analysis taking account of the judgments in *Fashion ID* and *Wirtschaftsakademie*). The paper also discusses the compliance issues that arise in relation to transparency and the rights of access, the completion of data protection impact assessments, special categories of personal data and joint controllership.		
ESMA publishes guidelines on outsourcing to cloud service providers	The European Securities and Markets Authority ("**ESMA**") released its guidelines around outsourcing to cloud service providers. Competent authorities and firms are obliged to comply with the guidelines (Article 16(3) ESMA Regulation). The guidelines aim to: – establish consistent, efficient and effective supervisory practices within the European System of Financial Supervision; – assure a common, uniform and consistent approach to applying aspects of relevant EU legislation (as outlined in the Guidelines) when firms outsource to cloud service providers; and – help firms and competent authorities with identifying, addressing and monitoring risks and challenges posed by cloud outsourcing arrangements, for instance regarding:	10 May 2021	Guidelines

Development	Summary	Date	Links
	– making the decision to outsource; – choosing a cloud service provider; – monitoring outsourced activities; and – providing exit strategies. The guidelines come into force on 31 July 2021. They will apply to all cloud outsourcing arrangements entered into, renewed or amended on or post-31 July 2021. Firms have until 31 December 2022 to amend existing cloud outsourcing agreements to ensure they are harmonised with the guidelines. When a cloud outsourcing agreement is not harmonised with the guidelines on or before 31 December 2022, in limited circumstances firms can inform their competent authority of this, along with proposed harmonisation measures/possible exit strategy from the agreement.		
EDPB adopts Opinions on transnational Codes of Conduct regarding cloud service providers	The EDPB adopted two Article 64 GDPR Opinions on the first draft decisions on 'transnational' Codes of Conduct (i.e. those that relate to processing activities in several Member States). Both of the draft decisions, which come from the French and Belgian supervisory authorities, are relevant to cloud service providers. The Belgian SA's draft decision concerns the EU CLOUD Code of conduct, and the French SA's draft decision concerns the CISPE Code of conduct. These codes are designed to provide guidance and define certain specific requirements (under Article 28 GDPR) for relevant processors in the EU – they are not to be used in the context of international transfers of personal data. According to the EDPB, both draft codes comply with the GDPR, fulfilling its Article 40 and 41 requirements.	20 May 2021	Press release
European Parliament urges Commission to issue guidance on international data transfers	Members of the European Parliament voted in favour of a resolution urging the European Commission to issue clear guidelines on making data transfers compliant with the Court of Justice of the European Union's findings in *Schrems II*. Following a report initially published by its Civil Liberties Committee, the European Parliament adopted the resolution calling for the	20 May 2021	Press release

Development	Summary	Date	Links
	Commission to issue comprehensive guidance integrating the EDPB's recommendations for data transfers and the EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries (published in January), to provide a toolkit of measures to bring protections in line with the standards required by the GDPR. In addition, the European Parliament called for infringement procedures to be taken against the Irish Data Protection Commission ("**DPC**") for its failure to initiate enforcement under the GDPR, and expressed its disappointment with the decision taken by the DPC to initiate the Schrems court case instead of independently pursuing enforcement action and also criticised their long processing times (see more below).		
EDPB publishes 2020 Annual Report	The EDPB issued its 2020 Annual Report. Notable EDPB activities in 2020 included: – contributing to the European Commission's evaluation and review of the GDPR as required under Article 97 GDPR; – producing guidance around processing personal data in the context of the COVID-19 pandemic; – the *Schrems II* judgment, along with issuing guidance documents including a FAQ document and some Recommendations concerning the judgment; and – adopting the first Article 65 GDPR binding decision. The 2020 Annual Report also sets out its main objectives for 2021, which follow the priorities set out in the EDPB 2021-2023 Strategy.	2 June 2021	Executive summary Report
European Commission adopts new standard contractual clauses, including for international transfers out of EEA	The European Commission adopted two new sets of standard contractual clauses. One set is for controllers and processors under Article 28(7) GDPR; the other set is for the transfer of personal data to third countries (the "**Transfer SCCs**"). The new sets of clauses reflect updated requirements under the GDPR and the European Commission says they will offer more legal predictability to businesses in the form of an easy-to-implement template.	4 June 2021	Eversheds Sutherland briefing Press release Article 28 SCCs Transfer SCCs

Development	Summary	Date	Links
	The Transfer SCCs have attracted particular attention as a means of plugging a compliance gap brought about by the *Schrems II* judgment, but the Transfer SCCs in and of themselves are not sufficient to comply with the judgment. You can read our briefing on the Transfer SCCs here. Clauses issued by the European Commission are no longer automatically adopted in the UK post Brexit, and so currently these clauses only provide an adequate safeguard for transfers from EEA countries to countries without adequate protection. The ICO has announced that it is planning on issuing UK specific contractual terms this year. If the Transfer SCCs are an appropriate tool for your organisation's data transfers, you will need to audit all the data transfer agreements you currently have in place (internally and with third parties) and only then – where applicable – ensure that the body of those contracts are updated to refer to the Transfer SCCs, that the security annex is updated and that the Transfer SCCs are appended accordingly (and are complied with in practice). In terms of implementing the Transfer SCCs, there are three key dates to be aware of: – the Transfer SCCs can be used to safeguard transfers from the **27 June 2021** onwards. – the *existing* standard contractual clauses will not be repealed for another three months, on **27 September 2021**. Until that date, you have a choice of whether to use the existing standard contractual clauses or the Transfer SCCs to safeguard your transfers. After that date, you must use the Transfer SCCs. – lastly, where the existing standard contractual clauses are used to safeguard any transfers that continue beyond 27 September 2021, then these must be replaced by the Transfer SCCs by **27 December 2022**. The Article 28 SCCs serve a different purpose – they provide a ready-made annex which controllers and processors can *choose* to insert into contracts to meet the requirements of Articles 28(3) and (4) GDPR – which to date have commonly been addressed by		

Development	Summary	Date	Links
	organisations in their own different ways. Even though the Article 28 SCCs contain certain provisions that favour a particular party (controller or processor), they generally present a balanced position and are optional. So whilst the clauses provide a useful benchmarking tool, we expect many organisations to continue using their own precedents when negotiating data processing clauses using in order to secure more favourable terms.		
EDPB adopts final recommendations on supplementary measures for data transfers	The European Data Protection Board published the final version of its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("**EDPB Recommendations**"). The EDPB Recommendations are designed to be read in tandem with the new Transfer SCCs and set out a six step plan to help organisations assess third countries and identify appropriate supplementary measures to be implemented on a case by case basis where needed. The EDPB also released an infographic which provides a illustrative summary of the necessary steps. The EDPB updated the recommendations (which were originally published in November 2020) to reflect the European Commission's position on organisations being able to considering practical experience of public authorities' access to personal data. In summary, if "problematic legislation" or practices are identified in the destination country which impinge on the effectiveness of the appropriate safeguards of the transfer tool(s), the EDPB now recommends the exporter to consider whether the laws/practices will be applied in practice to the relevant data, taking into account the importer's experience and sector.	21 June 2021	Recommendations Infographic
EDPB and EDPS adopt joint Opinion calling for ban on use of AI for AFR in public spaces	The EDPB and EDPS adopted a joint Opinion on the European Commission's Proposed AI Regulation. Among other things, the Opinion expresses concern over the exclusion of international law enforcement cooperation from the proposal. In addition, the EDPB and EDPS call for the proposal to be amended so the concept of "risk to fundamental rights" is aligned with the EU data protection framework as well as a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, (including recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other	21 June 2021	Press release

Development	Summary	Date	Links
	biometric or behavioural signals, in any context). The EDPB and EDPS also consider that data protection authorities should be designated as national supervisory authorities (pursuant to Article 59 of the proposal) to help ensure the regulation is applied consistently.		
EDPB publishes leaflet on consistency and the one-stop-shop	The EDPB has published a leaflet on consistency and the one-stop-shop under the GDPR. The one-stop-shop is a system of cooperation between national data protection authorities which helps individuals to enforce their rights and reduces the administrative burden on organisations. National data protection authorities can communicate with each other in order to investigate potential breaches of data protection rights.	29 June 2021	EDPB leaflet

Austria

Contributors

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

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

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

Development	Summary	Date	Links
Constitutional Court holds that government cannot rely on data protection to refuse parliamentary investigation committee's disclosure request	The Austrian Constitutional Court had to rule on two disputes between government and parliament, where an investigation committee had been tasked with examining possible corruption in Austria's last centre-right government. During its investigation, the committee discovered video footage of the former vice-chancellor offering government contracts in exchange for political and media support. The committee requested thousands of documents from several ministries and the chancellery, including several full e-mail accounts. The government refused to disclose these, relying on – among other reasons – the civil servants' privacy. Finding the balance between the parliamentary investigation committee's authority and these privacy concerns, the Constitutional Court decided that any disclosure request covered by the object of investigation cannot be refused based on data protection concerns (there are procedural rules for confidential information).	21 May 2021	Link to decision 1 (German) Link to decision 2 (German)
Federal Administrative Court finds retention of passport data in central ID register unlawful	An Austrian citizen filed a complaint against a local authority regarding its practice of retaining photos from passport applications in excess of mandatory retention periods. The authority justified its passport photo retention period by referring	25 June 2021	Link to decision (German)

Development	Summary	Date	Links
	to its additional administrative functions, e.g. as lost property office. The court ruled that such additional functions cannot be used as a lawful basis under the GDPR to prolong passport photo retention, and the local authority had therefore breached the GDPR's purpose limitation principle.		
Federal Administrative Court finds tax-information exchange does not infringe privacy law	An Austrian resident filed a complaint against the tax authorities regarding the exchange taxation data (specifically data about the complainant's bank account in Germany). The complainant argued that the information exchange between tax authorities based on Directive 2014/107/EU was an infringement of their privacy (referencing the CJEU rulings in *Digital Rights Ireland* and *Schrems*), contained special category data and was excessive in including specific bank account details. Furthermore, the complainant argued that the information exchange system was insufficiently secure and that a DPIA had been required but was not been conducted. Additionally, the complainant applied for a CJEU preliminary ruling. Both the Austrian and the German data protection authorities dismissed the complaint. The Federal Administrative Court dismissed the complainant's appeal, stating that there was no individual right to a controller conducting a DPIA or implementing specific security measures under Article 5 GDPR. Contrary to popular belief in Austria, financial and tax information do not fall under the definition of special category data. Moreover, the information exchange as required by EU legislation is a sufficient lawful basis for the data processing by tax authorities. A preliminary ruling was not necessary.	25 June 2021	Link to decision (German)

China

Contributors

Jack Cai
Managing Partner
T: +86 21 61 37 1007
jackcai@
eversheds-sutherland.com

Sam Chen
Of counsel
T: +86 21 61 37 1004
samchen@
eversheds-sutherland.com

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

Development	Summary	Date	Links
Second draft of the Personal Data Protection Law **《个人信息保护法(草案二次审议稿)》**	On 29 April 2021, the Standing Committee of the National People's Congress of China published the second draft of the Personal Data Protection Law ("**Draft PDPL**") for public comments. We summarise below the material changes in the second draft of the Draft PDPL compared to the first draft. *Specific obligations on specific data processors* The Draft PDPL imposes specific obligations on data processors who process a "significant amount" of personal data for online users, organisations that have a "complex business type" as well as organisations that provide "basic Internet platform services". These obligations include: establishing a new independent supervisory body responsible for the supervision of data privacy, regularly publishing reports on the organisation's compliance with data protection obligations, and to stop servicing the products of service providers that have seriously violated laws and regulations. *Legal basis for processing personal data* The Draft PDPL adds one legal basis for processing personal data, which is the processing of publicly available information within a reasonable scope.	29 April 2021	Second draft of the Personal Data Protection Law

Development	Summary	Date	Links
	Standard contract for cross-border transfer The Cyberspace Administration of China ("**CAC**") will provide a standard contract for data processing when entering into contracts with recipients outside of China. *Data protection rights of deceased persons* The scope of subjects with data protection rights has been expanded to deceased persons, whose rights under the Draft PDPL may be exercised by "near relatives" of the deceased on their behalf.		
Draft interim measures on the administration of personal data protection on mobile internet applications **《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》**	On 26 April 2021, the Ministry of Industry and Information Technology published the draft interim measures on the administration of personal data protection on mobile internet applications ("**Draft Measures**") for public comment. The Draft Measures specify various requirements and obligations for mobile application developers, distribution platforms, third-party app service providers, mobile device manufacturers and network access service providers. – Jurisdiction – the Draft Measures only apply to the processing of personal data in China collected via Apps used within China. – Principle of 'informed consent' – those who engage in the processing of app personal data shall inform users of their processing rules clearly so that any consent by users is voluntary and fully informed. – Principle of 'minimum necessary use' – other than the collection of personal data which is necessary for providing basic functions, collection of personal data must be optional. – Liabilities – any app which fails to rectify its violation of the Draft Measures will be removed from app stores for at least 40 working days and may possibly be blocked from internet access indefinitely.	26 April 2021	Draft interim measures on the administration of personal data protection on mobile internet applications
Data Security Law 《数据安全法》	On 10 June 2021, the Standing Committee of the National People's Congress of China passed the Data Security Law ("**DSL**"). The DSL will take effect on 1 September 2021.	10 June 2021	Data Security Law

Development	Summary	Date	Links
	Jurisdiction and scope The DSL applies to any data processing activities carried out within the territory of the People's Republic of China ("**PRC**"), as well as data processing activities outside the PRC that damage the national security, public interest and lawful interests of citizens/entities in China. "Data" is widely defined as any information that is recorded in electronic or other forms. *Categorical and hierarchical data protection system* The DSL establishes a categorical and hierarchical data protection system, which requires data to be classified and protected based on: i) the importance of the data to economic and social development; and ii) the degree of harm imposed on national security, public interest or the legitimate interest of citizens/entities in the event that the data is distorted, destroyed, leaked, illegally obtained or illegal utilized. *"Important data" and "national core data"* National core data is defined as any data concerning national security, national economic lifeline, people's fundamental livelihood, and major public interests. The DSL does not define important data but provides that the "important data" catalogue will be issued by the relevant authorities. Both important data and national core data will be subject to stricter administration. *Key protection obligations of data processors* These include: establishing comprehensive data security management systems, strengthening risk monitoring, taking remedial actions when data security defects or loopholes are detected and cooperating with relevant authorities for the purposes of protecting national security and investigating crime. *Cross-border data transfer* The DSL establishes a separate framework for cross-border transfers of "important data" by Critical Information Infrastructure ("**CII**") operators and ordinary network operators. The cross-border transfer of important data by CII operators are subject to the provisions of the Cybersecurity Law of China. The cross-border transfer of important data by other data processors will be subject	Effective date: 1 September 2021	

Development	Summary	Date	Links
	to the rules to be made by the CAC and other relevant departments of the State Council. As the provisions of the DSL are largely principle-based, we expect that further implementing rules will be introduced in the future.		
Draft provisions on the administration of automobile data security **《汽车数据安全管理若干规定（征求意见稿）》**	On 12 May 2021, the CAC released a draft of several provisions for the administration of automobile data security ("**Draft Provisions**") for public comments. The Draft Provisions govern data collection and processing activities in relation to all operators in the automobile industry and some related sectors. The types of data subject to the Draft Provisions are: 1) personal data, which includes personal data of car owners, drivers passengers and pedestrians as well as any information which can infer personal identity or describe individual behaviour, and 2) "important data" such as data on the flow of people and vehicles in military administrative zones, and audio and video data captured outside a vehicle. The Draft Provisions set out five principles for the processing of personal data and important data, which are: 1) non-collection of data as the default setting; 2) in-car processing (i.e. limiting information provided as far as possible to that within the car); 3) data anonymisation (if processing of information outside of the car is necessary); 4) minimum retention period; and 5) applicable scope of precision. The Draft Provisions provide that personal data and important data (as defined above) must in principle be stored in China, and if it is necessary to transfer data overseas, it must pass the CAC's cross-border data transfer security assessment. If there is an overseas transfer of personal data involving more than 100,000 people or important data, operators will be subject to extra compliance obligations, including filing annual reports to the relevant cybersecurity authority.	12 May 2021	Draft provisions on the administration of automobile data security

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

Emmanuel Ronco
Partner
emmanuelronco@
eversheds-sutherland.com

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

Edouard Burlet
Associate
edouardburlet@
eversheds-sutherland.com

Development	Summary	Date	Links
End of grace period for new cookie regulations	On 1 October 2020, the CNIL published new guidelines and recommendations regarding cookies and similar trackers. The CNIL granted website operators 6 months to bring their websites into compliance with the new rules. This grace period ended on 31 March 2021. In its statement dated 2 April 2021, the CNIL reminded website operators that they must, as of 31 March 2021: – clearly inform website users about all the purposes for which cookies are used on the website at the time they are presented with the option to accept or refuse the cookies; – ensure that acceptance to cookies is explicit, e.g. a button clearly stating "I accept" on which the user clicks would be acceptable (continuing to browse a website can no longer be considered as consent); – ensure that it is as easy to refuse the cookies as it is to accept them (either by including a "Refuse all cookies" button in the	2 April 2021	CNIL's statement (in French)

Development	Summary	Date	Links
	cookie banner, or by clearly indicating that closing the cookie banner would be regarded as a refusal of the cookies). The CNIL also indicated that it will assess whether cookie walls can be considered lawful on a case-by-case basis, including by examining whether the website operator offers alternatives for the service. The CNIL warned that it would start conducting controls to verify compliance with the new cookie rules, and would use all the means at its disposal (which include issuing formal notices or sanctions) if it identifies infringements.		
FAQ on use of saliva tests for COVID-19 in French schools	The French Ministry of Education launched test campaigns in French schools to prevent the spread of COVID-19 among students and teachers. On 23 April 2021, the CNIL issued a FAQ relating to the use of saliva tests on students. It is to date the first statement of the CNIL relating to the use of such saliva tests for COVID-19 in France. The CNIL underlined that it is not mandatory for students to undertake saliva tests. Parents and children have to be informed prior to the launch of a testing campaign in their schools, and parents can refuse that their children be tested. Children who do not undertake a saliva test must still be allowed to enter the school premises. The CNIL indicated that only the personal data necessary for the performance of the test (basic information on the child, including his or her social security number, and contact details of the parents) may be collected. No other information may be collected or retained (for example on the symptoms experienced by the child). The data that is collected and the test results may only be processed by the laboratory and the health authorities, and only the parents are informed about the result of the test. The parents should then inform the school to allow the director to handle the risks of contamination of other students or school personnel.	23 April 2021	CNIL's statement (in French)
Recommendations on measures to protect against ransomware	In light of the significant increase of ransomware attacks against private companies, public bodies and healthcare establishments, the CNIL issued best practice guidance designed to limit such attacks and the associated risks. The guidance is based on experience of	30 April 2021	CNIL's statement (in French)

Development	Summary	Date	Links
	previous attacks as well as recommendations of the French National Agency for the Security of Information Systems. The CNIL recommends implementing the following measures when a ransomware attack is identified: – turning off all devices; – immediately informing the IT department; – avoiding paying the ransom; – keeping all evidence (including the logs, the encrypted data, etc.); and – filing a complaint with the police. The CNIL also underlined that appropriate security measures should be taken in any case to ensure compliance with article 32 GDPR, and in particular the following measures to reduce the risk of a ransomware attack: – maintaining and regularly updating "offline" backups; – segmenting IT systems; – raising staff awareness regarding security risks and the actions to be taken in case of a security breach; – regularly updating the antivirus, browser and operating software, etc.; and – implementing appropriate procedures to identify significant security breaches. Finally, a security breach must be notified to the CNIL in accordance with the GDPR, when personal data is involved and there is a risk to the rights and freedoms of the data subjects. This is the case when the ransomware encrypts the data and exports it to the attacker's system.		
New reference document for identification of employees who commit road offences with company vehicles	The CNIL announced its adoption of a new reference document on the identification of drivers who have committed road traffic offences with company-owned vehicles. The reference document is aimed at public and private entities who provide their employees with company cars, and to car rental	CNIL's statement: 30 April 2021	CNIL's statement (in French) CNIL's deliberation (in French)

Development	Summary	Date	Links
	agencies. Such entities receive the tickets for road traffic offences committed with their vehicles, and can then contact the public authority in charge of the processing of such tickets to provide the name of the driver responsible for the offence. The CNIL's reference document lists the legal bases that can be used to justify such processing of personal data, as well as the categories of personal data that can be processed. In particular, even though personal data relating to criminal offences and convictions can be processed only in limited circumstances, the CNIL underlines that the processing of such data is justified in the above-explained circumstances in accordance with the provisions of the French Highway Code. The CNIL however warns that such data can only be shared with a limited number of recipients, in particular public entities, and can be retained only for a limited period of time, which may generally not exceed 45 days. In addition, a data protection impact assessment may be required in some circumstances, in particular if the processing of data for the identification of offenders is implemented by a company which has more than 250 employees or by a car rental agency conducting large scale processing activities. The reference document also states that the above-mentioned entities may use anonymous statistics about road traffic offences, notably in order to be able to provide their employees/customers with relevant road safety trainings.	CNIL's deliberation: 12 April 2021	
CNIL 2020 annual report	The CNIL published on 18 May 2021 its activity report for the year 2020. The CNIL focused on the protection of personal data in relation to the COVID-19 pandemic, which gave rise to an increase use of distance communication technologies and tracing tools to try to prevent the epidemic. It also worked on updating its recommendations and guidelines on cookies to ensure compliance with the GDPR and a better protection of data subjects. The CNIL also indicates that it:	18 May 2021	CNIL's report (in French)

Development	Summary	Date	Links
	– received over 13,500 complaints (an increase of 62,5% from 2018); – received over 2,800 data breach notifications (a 24% increase from 2019); – carried out 247 inspections and issued 14 sanctions, including 11 administrative fines for a total amount of over EUR 138 million; – issued 49 formal notices; and – worked on over 1,000 cases in cooperation with other EU data protection authorities.		
CNIL reference document for rental management activities	In November 2020, the CNIL launched a public consultation on the draft reference document it had prepared about rental management. On 27 May 2021, the CNIL publicly announced that it adopted on 6 April 2021 the final version of this reference document, which includes the inputs received during the consultation. The CNIL's reference document is directed to natural persons or legal entities renting residential premises, but also to professionals acting as lessors' representatives or involved in operations relating to another person's premises, and to online platforms offering services relating to rental management. The reference document 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. It lists the categories of personal data that can be collected, the legal bases that can be used, the recipients with whom the personal data of tenants or prospective tenants may be shared, as well as the retention period for such data. This reference document is not prescriptive, it aims at guiding professionals in bringing their activities in line with data protection laws and in conducting a data protection impact analysis where necessary. However, professionals may depart from the CNIL's guidelines if they are able to justify their decisions to do so.	CNIL's statement: 18 May 2021 CNIL's deliberation: 6 May 2021	CNIL's statement (in French) CNIL's deliberation (in French)

Development	Summary	Date	Links
Public consultation CNIL draft recommendation about log files	On 28 May 2021, the CNIL issued its draft recommendation on the use of log files and launched a public consultation on this draft. Keeping log files is an important measure to ensure that personal data processing operations are appropriately protected in accordance with the GDPR. Log files can help investigate and identify the source of an incident, an intrusion in databases or a misuse of personal data. However, log files also contain personal data about the users of the IT system, including their identifiers, the date and hours of their connections to the system, etc. Such data may, for example, provide information about their professional performance. The CNIL's draft recommendations contain guidance on the categories of personal data that may be collected in relation to log files and the period during which such data may be retained. As a general rule, the CNIL recommends to keep this data for a period ranging between 6 months and 1 year. It indicates that it deems such duration to be sufficient to ensure that log files may be used in case of security breaches while complying with the GDPR principle on limited retention periods. The CNIL also indicated that a longer retention period may be justified in certain circumstances, and provides guidance on the criteria (e.g. the specific risks for data subjects in case of a security breach, the legal obligations applicable to the controllers) to take into account when determining the appropriate retention duration. The public consultation on the draft recommendations is open until 23 July 2021.	28 May 2021	CNIL's statement (in French)
Opinion of the CNIL on the tools that can be used to prevent the spread of the COVID-19 epidemic	On 8 June 2021, the CNIL issued several statements regarding the tools that can be implemented against the spread of COVID-19 and the data protection rules to be complied with in relation thereto. The CNIL in particular commented on: – The records to be implemented by several categories of establishments open to the public, including restaurants, bars and sport facilities, for contact tracing purposes.	8 June 2021	First CNIL's statement (in French) Second CNIL's statement (in French)

Development	Summary	Date	Links
	According to the rules issued by the French government, such establishments must record information about their clients, either in a paper record or by scanning the QR codes that their clients may obtain on the contact tracing app operated by the French government. Such records can then be used, if a customer is tested positive to COVID-19, to inform other customers that they may have been exposed to the virus, so that they can self-isolate and undertake COVID-19 tests accordingly. – The CNIL has in particular provided recommendations about how paper records can be used for contact tracing purposes. In particular, it has indicated that only a limited number of information may be included in such records (i.e. the name of the customer, their phone number and the date and time of arrival), that a privacy notice should be provided to the customers, and that the information contained in the record must be deleted after 15 days. In addition, such information cannot be used for any purpose other than contact tracing (e.g. direct marketing) and cannot be shared with anyone other than public health authorities. – A "health pass" can be obtained with either: (i) a negative PCR or antigenic test; (ii) a vaccination certificate; or (iii) a medical certificate indicating that the individual has recently had COVID-19. According to the health regulations applicable since June 2021 in France, this digital health pass is required for access to premises which can receive over 1,000 people (such as concert halls) or open-air events with more than 1,000 attendees. When a verification of the health pass is required, individuals can use either the COVID-19 app or any other digital or paper document including their test results or vaccination/medical certificates. – The CNIL has notably clarified that, when the COVID-19 app is used to display the health pass, the persons carrying out the verifications shall only access names, birth dates and confirmation that the health pass is valid, and no other information about the individual whose pass is verified (e.g. they cannot know whether this individual has taken a COVID-19 test or has been vaccinated). The CNIL further underlines that, when paper documents are used as health passes, the persons whose passes are checked should be able to only present the		

Development	Summary	Date	Links
	information necessary for the control of the validity of the passes, in order to comply with the data minimisation principle.		
Recommendations of the CNIL to better protect minors online	In 2020, the CNIL started a public consultation regarding the protection of personal data of minors. The CNIL later announced in January 2021 that it had launched an internal deliberation on how to protect minors online. Following this discussion, it has issued on 9 June 2021 eight recommendations, to provide appropriate protection to minors whilst taking into accounts the need for autonomy they may have passed a certain age. The CNIL underlines that minors may use different types of platforms and websites, including social media and gaming platforms, which can involve the collection of large amounts of information about their identity, their preferences and lifestyle. Minors must be particularly protected because of the potential impact that the processing of their personal data may have on their educational experience or future careers. The CNIL emphasises that different rules should apply depending on the age of the minors. It is not possible to have identical rules for a 6-year-old and a 16-year-old, for example. The CNIL's recommendations therefore aim at taking into account the need to protect the privacy of children, but also the minors' need for autonomy, while giving parents an important role in the supervision of their children's online activities. The CNIL's recommendations include: – regulating minors' online activities (e.g. ensuring that the online services available to minors are adapted to this public and strictly comply with the data protection rules regarding minors); – encouraging minors to exercise their rights (in particular on social media, video sharing and gaming platforms); – supporting parents in providing digital education to their children; – seeking parental consent for minors under 15 (to ensure compliance with French data protection law which requires a joint consent of the minor and at least a parent before any	9 June 2021	CNIL's statement (in French)

Development	Summary	Date	Links
	processing of personal data of the minor which relies on consent); – promoting parental control tools that respect children's privacy and interests (e.g. such tools must not allow for the real-time geolocation of the minors); – reinforcing the information of minors and their rights through adapted design (e.g. having privacy notices understandable for minors and that include a specific section on the protection of minors' personal data); – verifying the age of minors and the parents' consent in a manner that protect their privacy (i.e. ensuring proportionality and data minimisation while still having strong processes for age verification for the most intrusive processing activities such as profiling); and – providing specific guarantees to minors to protect their interests (e.g. avoiding that profiling be activated by default). The CNIL finally indicates that it may issue more practical advice on some of these recommendations after conducting additional consultations with the relevant stakeholders.		
Approval of the first European code of conduct for IaaS providers	The CNIL formally approved the code of conduct elaborated by Cloud Infrastructure Service Providers Europe, intended for cloud infrastructure service providers located in the European Union. The CNIL's formal approval follows the adoption on 19 May 2021 of the EDPB's "Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)", in which the EDPB considered that CISPE's code of conduct complies with the GDPR. The code of conduct is divided into several parts: – a description of its material and geographical scope of application; – the requirements regarding protection of personal data; – the requirements regarding security measures;	CNIL's statement: 9 June 2021 CNIL's deliberation: 3 June 2021	CNIL's statement (in French) CNIL's deliberation (in French) Code of conduct

Development	Summary	Date	Links
	– the modalities to adhere to the code of conduct; and – the monitoring mechanisms. In accordance with Article 41 GDPR, the monitoring of compliance with the code of conduct will, without prejudice to the tasks and powers of the CNIL, will be carried out by the bodies identified by CISPE (when they will have received accreditation for the CNIL).		
Administrative fine of EUR 500 000 for infringements of GDPR and ePrivacy regulations	On 14 June 2021, the CNIL issued an administrative fine of EUR 500 000 against a company specialising in the online sale of DIY, gardening and home decor products. The CNIL had carried out three inspections between 2018 and 2021 of the company's website and identified several infringements of data protection and ePrivacy rules: – failure to limit the retention period of the personal data: The CNIL found that the company was retaining the personal data of over 16 000 clients who had not placed any orders for more than 5 years, as well as the personal data of more than 130 000 who had not logged in their account for more than 5 years. – failure to provide transparent information: The information available on the company's website (i.e. the general terms of sales and the privacy notice) did not include all the requirements listed in the GDPR. In particular, the contact details of the DPO, the retention periods for the personal data, the legal bases for the data processing operations as well as some of the rights of the data subjects were not mentioned in the information notices. – failure to comply with erasure requests: The CNIL found that the company had not deleted the personal data of the individuals who requested the erasure of such information in accordance with the GDPR, but only deactivated their accounts. – failure to appropriately protect personal data: Several basic security measures were not implemented – customers could create passwords that were not strong enough, the passwords of all employees for access to the company's database were all listed in a single document, and a shared account was used for the access to the company's database.	CNIL's statement: 9 June 2021 CNIL's deliberation: 14 June 2021	CNIL's statement (in French) CNIL's deliberation (in French)

Development	Summary	Date	Links
	– failure to obtain valid consent for direct marketing by e-mail: The CNIL identified an infringement of the ePrivacy regulations during its inspections, since it noted that direct marketing messages were sent to individuals who had created an account on the company's website, but had not provided consent or made any purchase. – failure to obtain consent to cookies: The CNIL also found that, when users of the company's website accessed the website, several cookies (including advertising cookies) were placed on their devices before they provided any consent. The company is based in France but also operates in three other EU countries: Spain, Italy and Portugal. The CNIL therefore consulted the data protection authorities of these three countries before issuing a sanction. In light of all the infringements that it had identified, the CNIL decided to impose an administrative fine of EUR 500 000. It also ordered the company to bring its processing activities in line with the ePrivacy rules and the GDPR within 3 months, and in particular to delete personal data that was too old, to implement an appropriate archiving system, and to stop sending direct marketing messages to customers who had not provided consent, failing which the company would have to pay a fine of EUR 500 per day of delay.		
CNIL recommendation on the exercise of data protection rights through a proxy	In November 2020, the CNIL launched a public consultation on the draft recommendation it had elaborated on the exercise of data protection rights through a proxy. On 25 June 2021, the CNIL publicly announced that it adopted on 27 April 2021 the final version of this reference document, which includes the inputs received during the public consultation. The CNIL's 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 French data protection law. This recommendation is directed to companies acting as proxies of data subjects, but also to controllers who receive right requests from companies appointed as representatives of data subjects. The	CNIL's statement and FAQ: 9 June 2021 CNIL's deliberation: 27 May 2021	CNIL's statement (in French) CNIL's FAQ (in French) CNIL's deliberation (in French)

Development	Summary	Date	Links
	recommendation will not be prescriptive, but could be used as a practical guide by such entities. The 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 right 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 by submitting an application for the exercise of right on behalf of a data subject. The recommendation also includes a template power of attorney that proxy companies and controllers can refer to. The template only contains provisions relating to data protection, and may be completed with commercial provisions, provided they do not contradict the applicable data protection provisions. In response to its consultation, the CNIL has also prepared a FAQ document addressing the practical issues that may arise when data protection rights are not exercised by the data subjects themselves.		
CNIL begins verifying website compliance with new cookie regulations	On 25 May 2021, the CNIL publicly announced that it had sent formal notices to around twenty companies that were not compliant with the new regulations on cookies and similar technologies. The CNIL found that the companies did not enable the users of their websites to reject cookies in an easy manner, whilst the new regulations require that refusing cookies must be as easy as accepting them. On 29 June 2021, the CNIL announced that it has closed the proceedings initiated against all the organisations that had received formal notices, since they have all brought their processing activities in compliance with the applicable cookie regulations.	29 June 2021	CNIL statement (in French)

Development	Summary	Date	Links
	The CNIL also underlined that it would continue to carry out verifications and to implement sanctions against companies that do not comply with the cookie rules in coming months. The CNIL has already noted those companies operating websites with a high rate of traffic and are not yet compliant with the new cookie regulations, and warns that it may issue further formal notices.		

Germany

Contributors

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

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

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

Jeanette da Costa Leite
Professional Support Lawyer
T: +49 89 54 56 54 38
jeanettedacostaleite@
eversheds-sutherland.com

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

Sara Ghoroghy
Senior 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
Hamburg DPA opines on possibility of consent to low-level technical and organisational measures	Article 32 GDPR requires the controller to take sufficient technical and organisational measures ("**TOMs**") to protect personal data. It is unclear whether a data subject can consent to a lower level of protection (e.g. the visitor to a website who is to consent to processing in another EU country). This question is controversial and has not been clarified in court, to date. In the opinion of the Hamburg Data Protection Commissioner, such consent is possible in principle. However, two things are mandatory for this: first, an effective, transparent and voluntary consent and secondly, the controller must be able to provide sufficient TOMs in the absence	1 April 2021	Opinion (German only)

Development	Summary	Date	Links
	of consent. In other words, they must not rely on the data subject giving consent.		
Requirements for an assertion of a request for information by an authorised representative of the data subject	The Higher Regional Court of Stuttgart ruled that an original power of attorney must be submitted when a claim for information pursuant to the GDPR is asserted by an authorised representative appointed by the data subject. Thus, if a lawyer wants to assert a claim on behalf of his client, he must present the original power of attorney to the controller and may not transmit it electronically.	1 April 2021	Judgment (German only)
Requirements for compliant cookie banners	The Regional Court of Cologne defined precise requirements for effective cookie banners. In particular, the wording "By continuing to use the website, you consent to the use of cookies." is unlawful. In the court's view, this wording is not compatible with Section 15 (3) of the German Telemedia Act (TMG - Telemediengesetz), as it lacks the necessary consent. However, the mere continued use of the website cannot be seen as implied consent. Moreover, in certain cases, such as the creation of user profiles, an explicit consent of the data subject is required according to the case law of the Federal Court of Justice.	13 April 2021	Judgment (German only)
Requirements for data protection certification programmes	Article 42(1) GDPR provides that certification schemes shall serve to demonstrate that the GDPR is complied with in processing operations by controllers and processors. German Data Protection Conference ("**DSK**") has now published a document describing the minimum requirements that must be met by all certification schemes. For example, the certification scheme must specify which processing activities it is to be applied for and it is mandatory to consider data subjects' rights as certification criteria. All controllers can use the document to view the minimum requirements they must meet for certification.	16 April 2021	Guideline (German only)
No right of a data subject to demand action by the data protection authorities	The Berlin Administrative Court ruled that data protection supervisory authorities are independent in the performance of their duties. However, a data subject does not have a claim against the authority for a specific action. Thus, the supervisory authority sufficiently fulfils its duties if it investigates the facts after a complaint by the data subject due to insufficient response to his request for information, determines a GDPR violation and	21 April 2021	Judgment (German only)

Development	Summary	Date	Links
	then issues a formal warning against the controller. In principle, it is not obliged to impose a fine. This cannot be legally demanded by the data subject.		
Requirements for asserting the right to a copy of personal data	The Federal Labour Court ruled that a claim for the provision of a copy of e-mails pursuant to Article 15(3) GDPR is not sufficiently determined within the meaning of German civil procedure law if the e-mails (a copy of which is to be provided) are not precisely designated. In the context of enforcement proceedings, it must be unambiguous as to which e-mails the claim relates.	27 April 2021	Press statement (German only)
Requirements for the dismissal of a data protection officer	The Federal Labour Court (Bundesarbeitsgericht, BAG) referred a question to the Court of Justice of the European Union ("**CJEU**") for a preliminary ruling on whether the requirements of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) for the dismissal of a company data protection officer are in line with the GDPR. National data protection law regulates, in Section 38 (2) and Section 6 (4) BDSG, that an 'important reason' within the meaning of Section 626 of the German Civil Code (Bürgerliches Gesetzbuch, BGB) is required for the dismissal of a company data protection officer. Therefore, the dismissal of a data protection officer is subject to higher threshold than under EU law.	27 April 2021	Press statement (German only)
Fax use breaches the GDPR	According to the data protection supervisory authority of Bremen, the use of telefax violates the GDPR. While a few years ago fax was still considered a relatively secure method to transfer even sensitive personal data, this situation has changed fundamentally. This is because the sender can never be sure what technology is being used on the receiving end. Fax services usually do not contain any security measures to guarantee the confidentiality of the transmitted data and are therefore generally not appropriate for the transfer of personal data. For example, there is often a lack of adequate encryption mechanisms. For the transmission of personal data, alternative, secure methods should be used instead, such as end-to-end encrypted e-mails or conventional mail, as appropriate pursuant to the GDPR.	1 May 2021	Statement by authority (German only)

Germany

Development	Summary	Date	Links
Cross-border control of the data protection supervisory authorities to implement the Schrems II decision of the European Court of Justice	The German data protection supervisory authorities announced their intention to participate in a transnational, coordinated audit of international data transfers. This audit serves to implement the *Schrems II* ruling of the CJEU, according to which transfers to the USA may no longer take place on the basis of the EU-US Privacy Shield. Furthermore, the use of the standard contractual clauses for data transfers to third countries is now only sufficient with the use of effective additional measures if the review by the controller has shown that no equivalent level of protection for the personal data can be guaranteed in the recipient state. As part of the audit, the participating authorities will contact controllers and ask them to answer a questionnaire. Among other things, the questionnaire will cover the use of service providers for sending e-mails, hosting websites, web tracking, managing applicant data and the intra-group exchange of customer data and employee data.	1 June 2021	Press statement by Data Protection Authority of Hamburg (German only) Questionnaire for controllers (German only)
Safeguards for the transfer of personal data via e-mail	The DSK adopted an orientation guide with measures for the protection of personal data when transmitted by e-mail. The requirements are listed in concrete terms. For example, controllers who use public e-mail service providers should satisfy themselves that the providers offer sufficient guarantees for compliance with the requirements of the GDPR and in particular the relevant Technical Directive. In addition, the requirements for encryption and signature procedures are defined.	16 June 2021	Guideline (German only)

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

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

Katrina Shum
Trainee Solicitor
T:+852 2186 3204
katrinashum@
eversheds-sutherland.com

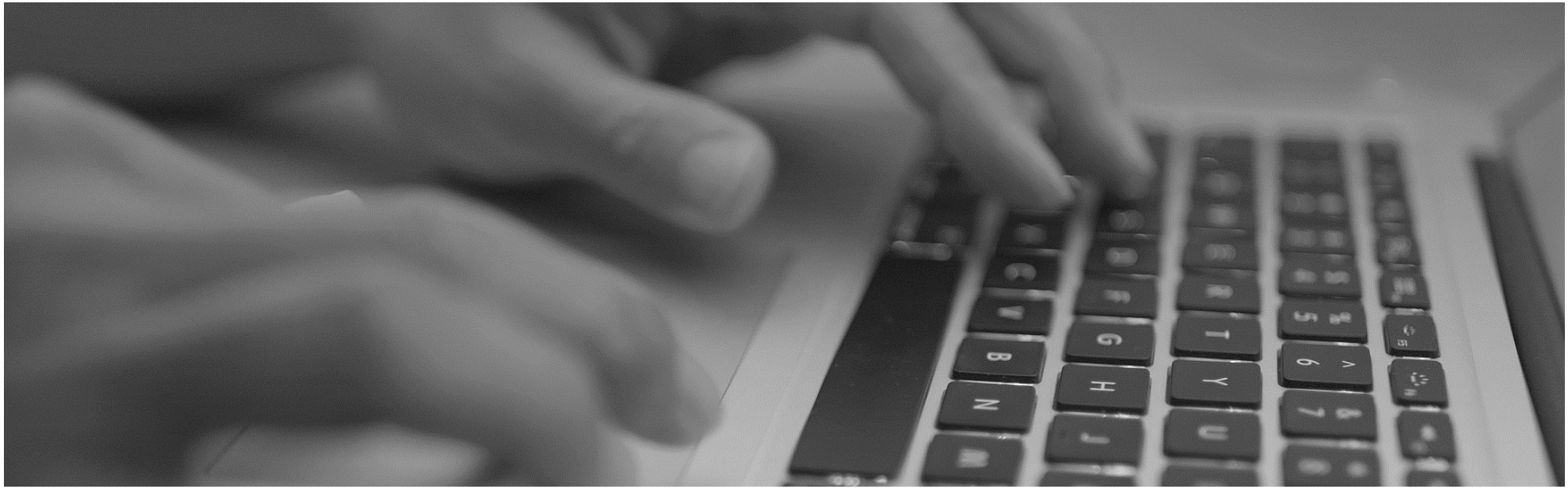
Woody Yim
Trainee Solicitor
T: +852 2186 3298
woodyyim@
eversheds-sutherland.com

Development	Summary	Date	Links
New PCPD guidance on personal data privacy and use of social media and instant messaging apps	In light of the digital footprint left (often inadvertently) by users of social media being prone to misuse by third parties for illegitimate purposes such as identity theft, cyberbullying or doxxing, the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") has issued guidance on the use of social media and instant messaging apps. The guidance recommends the users of social media to: – take steps to understand how social media platforms handle their personal data by examining the privacy policies;	5 April 2021	PCPD media statement Guidance

Development	Summary	Date	Links
	– regularly review their privacy settings to retain control over what information will be disclosed to other users and how widely the information is disclosed; – limit the permissions granted to social media platforms on how their personal data, such as facial images and location data, can be used; – think twice before they share or send any information on social media; – respect other people's privacy and be cautious about tagging other people in photos or sharing information about other people; and – be vigilant about online scams, such as malicious hyperlinks that request the users to "log-in" or provide personal data. A "Step-by-Step Guide on Adjusting Privacy Settings" is appended as an annex to the guidance which outlines the steps users can follow in order to adjust some common privacy settings via the operating systems of mobile phones, or by directly adjusting the settings in the social media apps.		
Proposed amendments to the Personal Data (Privacy) Ordinance to combat doxxing	Following the PCPD's media statement in expressing its intention to formulate concrete policies to combat doxxing, the Secretary for Constitutional and Mainland Affairs and PCPD have laid out their proposed amendments on the Personal Data (Privacy) Ordinance (Chapter 486, Laws of Hong Kong) ("**PDPO**") to the Legislative Council. The proposed amendments include: *Adding an offence to curb doxxing* – a new doxxing provision would be added to offer protection to the immediate family members of the data subject. – those contravening the new offence would be liable on conviction on indictment to a fine of HK$1,000,000 and to imprisonment of five years, or on summary conviction to a fine of HK$100,000 and to imprisonment for 2 years. Empowering the PCPD to carry out criminal investigation and prosecution	17 May 2021	Proposed amendments to the Personal Data (Privacy) Ordinance (Cap. 486)

Development	Summary	Date	Links
	– the PCPD could request relevant information and documents from any person or require any person to answer relevant questions to facilitate investigation when it has reasonable grounds to believe that a contravention of the doxxing offence(s) has been or is being committed. – proposed amendments to the provisions would allow the PCPD or any prescribed officer to apply for the court's permission for entry into any premises for doxxing offences. – the PCPD would be empowered to prosecute in its own name for cases of suspected contravention of a doxxing offence under the PDPO or failure to comply with the PCPD's requests related to criminal investigation. Conferring on the PCPD statutoy powers to demand the rectification of doxxing contents – the PCPD would be empowered to serve rectification notices on any person where it has reasonable grounds to believe a doxxing offence has been committed. – an appeal mechanism would be in place for aggrieved persons who are subject to rectification notices; however, such persons would have to first comply with the rectification notice within the designated timeframe pending the appeals board's final decision to contain the harm caused to the data subjects or their immediate family members. – new provisions would empower the PCPD to apply to the court for an injunction against doxxing acts targeting specific persons or groups if it is satisfied that there is, or it is very likely that there is, large-scaled or repeated contraventions of the doxxing offences of the PDPO in the society.		
New public inspection regime under the Companies Ordinance gazetted to widen access of corporate directors' data for professionals and deter money laundering	In view of rising community concern over whether personal information contained in public registers is adequately protected, the Hong Kong Government has considered it appropriate to implement a new inspection regime under the Companies Ordinance (Chapter 622, Laws of Hong Kong) ("**CO**") to enhance protection of personal information while ensuring that the public could continue to inspect the Companies Register under the CO.	18 June 2021	Government press release Legislative Council Brief

Development	Summary	Date	Links
	Under the new inspection regime, a longer list of "specified persons" (including practising accountants, lawyers and bankers) can gain access to certain protected information, namely the usual residential addresses and full identification number, of corporate directors and executives upon application to the Companies Register. It addresses the need to ensure the robustness of the financial, commercial and corporate governance systems of Hong Kong, and proper conduct of law enforcement. Meanwhile, the public's data access will gradually be limited to, among others, the correspondence addresses and partial identification numbers of corporate directors and other officers. The implementation of the new regime will be carried out incrementally in three phases and is expected to be completed by 27 December 2023.		



Ireland

Contributors

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

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

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

Development	Summary	Date	Links
European Parliament expresses disappointment with the DPC over handling of *Schrems II*	See update above. The European Parliament's resolution called for infringement procedures to be taken in response to Ireland's "lack of GDPR enforcement". The DPC's long processing times were criticised in addition to the DPC's decision to initiate the Schrems decision rather than independently triggering EU GDPR enforcement procedures.	20 May 2021	Press release
DPC Draft Regulatory Strategy for 2021-2026	The Irish Data Protection Commissioner ("**DPC**") published its Draft Regulatory Strategy for 2021-2026. The DPC seeks to give direction to its broad regulatory remit, while at the same time taking account of the needs of data subjects and organisations. This Draft Regulatory Strategy was published for the purpose of consultation with stakeholders, who were invited to make submissions to the DPC by 30 June 2021.	23 April 2021	Draft regulatory strategy
Joint Committee on Justice Debate – Discussion of Irish DPC Criticism	On 27 April 2021, the Irish government Joint Committee on Justice held a debate on GDPR attended by participants including Max Schrems and the Data Protection Commissioner, Helen Dixon. Criticisms were made of the DPC such as the low number of complaints resolved, it was alleged that the DPC had a poor understanding of procedural law and it was alleged that the DPC displayed a fear of litigation. The DPC agreed that improvements are required, particularly in relation to the speed of processing	27 April 2021	Full text of debate

Development	Summary	Date	Links
	and resolving complaints. The full text of the debate is available in the link provided.		
Chair of the EU Scrutiny Committee asks how the EU directive on the resilience of critical entities interacts with the protocol on Ireland/Northern Ireland	The EU Scrutiny Committee has requested clarification as to how the interests and concerns of all relevant government departments, regulatory bodies, administrations and external stakeholders will be accounted for in reaching an informed decision regarding regulatory alignment or divergence.	12 May 2021	Request
DPC publishes guidance in relation to individuals contacting organisations on behalf of someone else	On the 21 May 2021, the DPC published guidance in response to dissatisfaction from individuals regarding steps they must take when contacting an organisation on behalf of someone else. The DPC provides that data protection law does not prevent organisations dealing with an individual on behalf of another, and organisations must ensure a balanced and proportionate approach to security and identity verification measures. Controllers should consider what level of security is necessary in each situation.	21 May 2021	DPC guidance
DPC publishes guidance relating to when your personal data has been affected by a breach	At the end of May 2021, the DPC published guidance in relation to protecting your information from criminals who steal personal data. The guidance also discusses how to deal with phishing in addition to threats to extort money or information.	28 May 2021	DPC guidance
DPC guidance on processing COVID-19 vaccination data in the context of employment	In June 2021 the DPC published welcome guidance as to whether or not employers can gather COVID-19 vaccination status information from employees. The DPC provides that 'the processing of vaccine data is likely to represent unnecessary and excessive data collection for which no clear legal basis exists.' The guidance will, however, be subject to review should the public health advice and laws relating to the interplay between the virus and vaccination change.	30 June 2021	DPC guidance
DPC guidance on the collection of personal data prior to viewing a property	The DPC's June 2021 guidance on the collection of personal data prior to viewing a property emphasises the importance of the data minimisation principle. The DPC does not consider the extensive collection of personal data from prospective purchasers at the initial stages of advertising or hosting viewings of a property to be justified. In line with the principle of purpose limitation, personal data should only be collected for 'specified,	30 June 2021	DPC guidance

Development	Summary	Date	Links
	explicit and legitimate purposes'. Data controllers must be transparent as to the purpose(s) of data collection and any processing of personal data must have a legal basis.		
Irish government amends Data Protection Act 2018 to provide an express right of individuals to enforce third party beneficiary rights conferred on data subjects under SCCs	On 27 June 2021, the Irish government adopted the European Union (Enforcement of Data Subjects' Rights on Transfer of Personal Data Outside the European Union) Regulations 2021 to clarify an uncertainty relating to Irish law as a governing law under the new SCCs adopted by the European Commission. There were concerns as to whether Irish law could adequately recognise third party beneficiary rights because privity of contract rules apply in Ireland. The introduction of this Regulation clarifies any concerns by providing an express right of individuals to enforce third party beneficiary rights conferred on data subjects under binding corporate rules and under SCCs.	24 June 2021	Regulations full text

Netherlands

Contributors

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

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

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

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

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

Development	Summary	Date	Links
District Court of Limburg rules on data subject access request and the abuse of rights	On 2 April 2021, the District Court of Limburg ruled on a data subject access request and the concept of abuse of rights. The claimant had filed a data subject access request at four municipalities in the Province of South Limburg. All municipalities had informed the claimant, within one month of receiving the requests, that they would only be able to process his data subject access requests if the claimant would identify himself. The claimant did not identify himself and the municipalities kept referring to the letters stating that identification was required. The District Court of Limburg ruled that there had been an abuse of rights, because it appeared that the claimant had not submitted his requests with the objective of receiving information relating to the processing of his personal data. The District Court of Limburg considered that the claimant had submitted the data subject access requests for the sole purpose of starting procedures to obtain damages from the various controllers.	2 April 2021	Court ruling

Development	Summary	Date	Links
	Therefore, the District Court of Limburg declared the appeals of the claimant as inadmissible.		
Violation of GDPR does not automatically lead to compensation for damages	On 7 April 2021 the District Court of Gelderland ruled on a dispute between a claimant and a real estate agent which arose when the real estate agent's computer system was hacked and personal data of the claimant was compromised. The police investigated in a timely manner. Nevertheless, the claimant was convinced that the real estate agent had violated the GDPR, as his personal data had been retained for too long and that he suffered damages as a result. The District Court of Gelderland clarified that in this case one cannot simply claim damages as a result of the aforementioned breach. A breach under GDPR does not automatically lead to compensation, as there must be evidence that damage has occurred. According to the District Court of Gelderland, it is insufficient evidence for the person involved to claim to have suffered "distress" – particularly because no discontent was expressed at the time of the hack to indicate "distress". The alleged damage had not been substantiated and, for that reason, damages could not be awarded. The District Court of Gelderland has not been able to make a substantive assessment of whether the GDPR has been violated.	7 April 2021	Court ruling
Municipality of Enschede fined for WiFi tracking	The Dutch Data Protection Authority ("**DDPA**") imposed a fine of €600.000 on Dutch municipality because the municipality used Wi-Fi tracking in the city centre in a way that was not permitted. By means of Wi-Fi tracking, the municipality was able to track shoppers and people who live or work in the city centre. In 2017, the municipality decided to use sensors to measure the traffic in the city centre. For this purpose, the municipality hired a company that specializes in counting bystanders. Measurement devices were installed on high streets to detect the Wi-Fi signals from shoppers' mobile phones. Each phone was registered separately, with a unique code. An investigation by the DDPA at the municipality established that the privacy of citizens had not been properly safeguarded, because citizens could be followed without it being necessary. The DDPA concluded as the use of Wi-Fi tracking, that makes the tracking of individuals possible, is in	29 April 2021	DDPA statement

Development	Summary	Date	Links
	itself a serious violation under the GDPR, a fine of €600.000 is appropriate.		
DDPA imposes fine of €525.000 on website for non-compliance with EU representative requirement	The DDPA imposed a fine of €525.000 on a website, which aims to locate and connect family members. The website published the addresses and telephone numbers of individuals, often without their knowledge or consent. Furthermore, it proved very difficult for individuals to have their personal data removed, because the website operator had no legal representative in the EU. Not having a legal representative in the EU is a violation under GDPR and was ultimately the main reason for the DDPA to impose a fine. The DDPA imposed an order compelling the company to appoint a representative in the EU, subject to a penalty for non-compliance. The company had until 18 March 2021 to appoint a representative in the EU. If the company refused, it would be obliged to pay €20.000 for every 2 weeks that the order was not complied with, with a maximum of €120.000.	12 May 2021	DDPA statement
Maintenance company fined for breach of privacy of sick employees	The DDPA has imposed a fine of €15.000 on a maintenance company for multiple breaches in the processing of medical data of sick employees. The company kept track of the causes of the sick leave of its employees. Furthermore, the company's absence registration records contained highly sensitive information about the physical and/or mental health of employees, such as the names of illnesses, specific complaints and indications of pain. Moreover, the absence registration was not adequately secured. As it is not necessary for an employer to process this information for the re-integration of employees and as the security of the personal data was insufficient, the DDPA imposed a fine. However, the DDPA noted that the company has since ended the aforementioned violations.	19 May 2021	DDPA statement
DDPA launches updated data breach notification form	The DDPA updated its data breach notification form, with the aim of making it easier for organisations to report a data breach to the DDPA. The following functionalities and updates have been included:	1 June 2021	DDPA statement

Development	Summary	Date	Links
	– the form determines which questions are shown based on the answers you provide. This way only the questions that are relevant for the organisation have to be answered; – the form can be saved and the report can be finalized at any given time; – a template can be created for common data breaches or a data breach that occurs frequently in a short period of time.		
DDPA fines orthodontic practice due to unsecured patient website	The DDPA imposed a fine of €12,000 on an orthodontic practice for using an unsecured website to register new patients, putting their medical personal data and social security numbers at risk. The unsecured website of this orthodontic practice came onto the DDPA's radar after receiving a complaint about the orthodontic practice. As it concerned the processing of medical data, the DDPA regarded the complaint as a reason to investigate. The online form that new patients used to register, contained mandatory entry fields for different categories of personal data. The personal data that patients filled out, was then sent to the orthodontic practice via an unencrypted connection and the personal data was mostly related to minor patients. The DDPA concluded that the orthodontic practice had not taken adequate security measures to protect the personal data of their (minor) patients, and subsequently imposed the fine.	10 June 2021	DDPA statement
Dutch DDPA publishes guidelines for organizing strong internal supervision	The DDPA received feedback that data protection officers ("**DPOs**") are regularly: – not involved, or too late involved, in plans and procedures where personal data is being processed; – not receiving the right documents; or – are not given enough time to do what is expected of a DPO. The interpretation of internal supervision is not properly arranged in all organizations. Therefore the DDPA has published guidelines regarding the position and tasks of the DPO.' These guidelines include, amongst others, the following:	24 June 2021	DDPA statement

Development	Summary	Date	Links
	– the organization must involve the DPO at an early stage in the (further) development of products and services and record what happens with the recommendations of the DPO; – the DPO must be clearly visible within the organization, be directly approachable, without the intervention of others; – the organization must guarantee the independent position of the DPO; and – the DPO has a central position in contacts between the DDPA and the organization. In this position, the DPO must be aware of the DDPA's communication with the organization. However, the DPO has an independent position and therefore cannot speak on behalf of the organization.		

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
Draft legislation on conversion of paper documents into electronic documents and creation of electronic duplicates before the Russian Parliament	A draft bill regarding electronic documentation is currently before the Russian Parliament. The draft bill introduces a definition of "conversion" of an electronic document, which means the transformation of an electronic document by changing its format but preserving its structure and content. The draft bill also defines the conditions of equivalence of the converted electronic document to the original electronic document signed with an electronic signature. Requirements for the electronic document conversion procedure will be established by the Government of the Russian Federation, and with regard to organizations with activities regulated by the Bank of Russia, these requirements will be established with the Bank of Russia's cooperation. In addition, the draft bill provides: – rules for creating electronic and mnual/physical duplicates of documents, including a list of exceptions - documents with respect to which the creation of duplicates is prohibited (these include, for example, documents certifying identity or containing state secrets); – the procedure and time limits for storage of electronic documents and documents with respect to which electronic duplicates were created or conversion was carried out; – conditions for preservation of legal validity of electronic documents during their storage period;	31 May 2021	Text of the Bill (in Russian)

Development	Summary	Date	Links
	– requirements for persons carrying out activities of conversion, storage and creation of duplicates of electronic documents and the procedure for their performance of such activities; and – the licensing procedure for converting, storing and creating duplicates of electronic documents. This draft bill reflects the government's intention to introduce electronic document processes in Russia as soon as possible.		
Fines for illegal disclosure of "confidential information" set to increase	A draft bill, which has been signed by the President, is set to increase fines for illegal disclosure of confidential information which includes personal data, trade secrets, bank secrets, etc. The cap on administrative fines for individuals is to increase to RUB 10,000. For officials, the cap on administrative fines is to increase to RUB 50,000. Officials will also be subject to disqualification under the new bill. Further, the draft bill introduces administrative liability for legal entities which includes the imposition of a fine of up to RUB 200,000. The draft bill will come into force after its promulgation.	11 June 2021	Text of the Bill (in Russian)
Draft legislation may expand categories of information that must be monitored by social networks	A draft bill on the subject of social network information monitoring is currently before the Russian Parliament. The draft bill would oblige operators of social networks to monitor the following types of information: – ways and means of developing homemade explosives and devices, firearms, self-made or remade main parts of weapons, restoration of the combat properties of decommissioned weapons; and – public justification of unlawful actions against life, health, and the freedom of citizens Currently the types of information that social networks must monitor includes: – materials with abusive images of minors and announcements about their involvement in activities of a pornographic nature, as well as their involvement in illegal activities;	18 June 2021	Text of the Bill (in Russian)

Development	Summary	Date	Links
	– ways and means of developing, manufacturing and using narcotic drugs, psychotropic substances, etc; – methods of committing suicide; – promotion and organisation of gambling and lotteries; – retail sale of alcoholic beverages and alcohol-containing food products; – insult to human dignity and public morals; and – calls for mass riots, extremist activities, etc.		
A new bill will require IT giants to open offices in Russia	A draft bill has been adopted by the Russian Parliament, requiring the owners of information resources with a daily audience of more than 500,000 Russian users (such as Facebook and Twitter) to launch a branch, open a representative office or establish a subsidiary in Russia which will serve as the main point of interaction with the Russian IT supervision authorities. The draft bill provides for a set of measures to compel IT companies to observe Russian legislation. The measures include bans on the following: – distribution of advertising; – any payment activities; – search results; and – collection and cross-border transfer of the personal data of Russian citizens. The draft bill is now awaiting the President's signature. Once it is signed, it will come into force after its promulgation.	23 June 2021	Text of the Bill (in Russian)

Singapore

Contributors

Sharon Teo
Partner
T: +65 6637 8886
sharonteo@
gtlaw-llc.com

Phoebe Sim
Associate
T: +65 6361 9307
phoebesim@
gtlaw-llc.com

Development	Summary	Date	Links
PDPC's broad comparison between the EU GDPR's six legal bases for processing of personal data and the consent and exceptions to consent provisions under the PDPA	On 1 April 2021, the Singapore Personal Data Protection Commission ("**PDPC**") published an infographic on the broad comparison between: – the EU GDPR's six legal bases for processing of personal data; and – the consent and exceptions to consent provisions under the enhanced Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**") which came into effect on 1 February 2021. Under the EU GDPR, controllers can only process personal data when there is a legal basis to do so. In this regard, the EU GDPR provides for six legal bases, namely: (i) consent, (ii) contractual necessity, (iii) compliance with legal obligation, (iv) vital interests, (v) public interests, and (vi) legitimate interests. By comparison, section 13 of the PDPA provides that an organisation shall not collect, use or disclose personal data about an individual unless the individual gives or is deemed to have given consent to the collection, use or disclosure. Section 17 of the PDPA provides for exceptions where an organisation may collect, use or disclose personal data without consent and they are categorised as follows: (i) vital interests; (ii) matters affecting the public; (iii) public interest; (iv) legitimate interests; (v) business asset transaction; (vi) business improvement purposes; and (vii) research purposes. The infographic is colour-coded to reflect the correlation between the six legal bases under the EU GDPR and the consent and exceptions to consent provisions under the PDPA. It is developed by the PDPC to assist Data Protection Officers who are required to do mapping of the PDPA and the EU GDPR for the purposes of their internal compliance policies or programmes.	1 April 2021	Link to PDPC's Infographic

Development	Summary	Date	Links
PDPC finds bank entitled to refuse access to redacted data in outcome of section 28 (now section 48H(1)(a)) of the PDPA review application	The PDPC has found that a bank was entitled to invoke the evaluative purpose exception under the PDPA and therefore was not required to provide an individual (the "**Applicant**") with access to redacted data in its possession. The review application arose from the bank's refusal to proceed with the Applicant's request to provide him with an unredacted copy of its internal evaluation report relating to the Applicant's unsuccessful credit card application. The redacted data in the report pertained to opinion data auto-generated by the bank's artificial intelligence ("**AI**") algorithms. The bank's position was that they were not obliged to disclose the redacted data to the Applicant as that data constituted opinion data kept solely for an evaluative purpose, which is an exception to an individual's right of access under the PDPA. The PDPC thus had to consider whether the bank's internal evaluation report constituted the Applicant's personal data, and if so, whether the bank could rely on the evaluative purpose exception for its refusal. In its review, the PDPC clarified that the primary focus in determining whether the redacted data formed part of the Applicant's personal data remained whether or not he was identified or identifiable from the information. It was therefore not relevant that the redacted data was algorithmically generated. The PDPC was satisfied that the evaluation report constituted the personal data of the Applicant since it did in fact contain identifiable information about him. As to whether the exception would apply, the PDPC was satisfied that it would be applicable because the redacted data was an expression of opinion after data processing and was not a mere reproduction of data or a result of simple arithmetic operations. With the growing use of AI systems for business evaluations and assessments, the decision issued by the PDPC is instructive, particularly where data may include a combination of personal data and opinion data generated using AI algorithms.	Date of Decision: 1 April 2021 Published: 12 May 2021	Link to the decision
PDPC's new handbook on how to guard against common types of data breaches	On 24 May 2021, the PDPC, pulling from past data breach cases heard and decided by the PDPC, published a new handbook which highlighted the five	24 May 2021	Link to PDPC handbook

Development	Summary	Date	Links
	most common gaps in information and communications technology ("**ICT**") system management and processes. The PDPC identified: (i) coding; (ii) configuration; (iii) malware and phishing; (iv) security and responsibility; and (v) accounts and passwords as the five most common issues in ICT system management and processes. In this handbook, the PDPC also sets out its recommendations on the corresponding ICT good practices that organisations should put in place to prevent data breaches.		
The General Division of the High Court of Singapore clarifies the scope of an individual's right to bring a private action under the PDPA	Section 32(1) (now section 48O) of the PDPA provides that a person who suffers loss or damage directly as a result of a contravention by an organisation / a person of any of the specified provisions of the PDPA has a right of action for relief in civil proceedings in a court. As the PDPA does not define "loss or damage", the General Division of the High Court of Singapore (the "**High Court**") in *Bellingham, Alex v Reed, Michael [2021] SGHC 125* had to consider whether emotional distress or loss of control of personal data could amount to "loss or damage" for the purposes of the PDPA. The High Court found that section 32(1) should not apply where the alleged loss or damage was simply a loss of control over personal data since loss of control would be inevitable in a case of contravention and conferring a right of action in every such case would render the term "loss or damage" redundant. The High Court further found that the term "loss or damage" in section 32(1) should be limited to the heads of loss under common law, i.e., pecuniary loss, damage to property and personal injury including psychiatric illness. The High Court directed that remedies be sought through the PDPC instead in cases like this where the individual has no right of action under section 32 of the PDPA. This case is significant, being the first time the issue of the scope of a private action under section 32 was decided.	25 May 2021	Link to decision

Spain

Contributors

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

Celia Bouzas Gonzáles
Senior Associate
T: +34 91 429 43 33
cbouzas@
eversheds.es

Development	Summary	Date	Links
AEPD issues guide to data protection and labour relations	This guide has been published by the Spanish Data Protection Agency ("**AEPD**"), with the aim of offering a practical tool to help public and private organisations to comply with data protection and labour relations legislation. In Spain, the application of the General Protection Regulation and the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD) has led to a series of changes both in the rights of workers and in the collection and use of their personal data by employers. The guide also addresses issues that are being raised with increasing frequency, inter alia, (i) consultation by the employer of the employee's social networks, (ii) internal whistleblowing systems, (iii) the recording of the working day (where the right of the works council to be informed by the company of the parameters on which algorithms or artificial intelligence systems are based, including profiling, which may affect conditions, stands out, and (iv) the use of wearable technology as an element of control. The document begins by outlining the bases that legitimise the processing of personal data, the information that must be provided and the data protection rights which apply in a work environment. It also addresses the principle of minimisation, and reminds employers that the existence of an employment contract does not mean that the employer has a right to know and store any type of personal data about its employees. In addition to the duties of secrecy and security (that personal data should only be known by the person concerned and by those users of the organisation with the authority to use, consult or modify such	18 May 2021	Guide on Data protection, labor relations (in Spanish)

Development	Summary	Date	Links
	data), the document also sets out the limits of data processing in the personnel selection and hiring processes.		
AEPD issues guidance for notification of personal data breaches	This document is an update of the 'Guide for the notification of personal data breaches' previously published by the AEPD. The guide's objective is the effective protection of the rights and freedoms of individuals, the creation of a more resilient environment based on knowledge of the organisation's vulnerabilities and the guarantee of legal certainty by providing controllers with a means of demonstrating diligence in fulfilling their obligations. The guide begins by analysing what is a personal data breach and what is not, in the context of the European, national and sectoral regulatory framework. It then discusses when such a breach must be notified to the supervisory authority, within what timeframe, by whom, and what content that notification must include. With regard to the communication to the affected persons, the document sets out the cases in which it must be made, the content and the deadlines. The guide also provide advice as to how to simplify compliance with these obligations and, among other points, provides guidance on certain deadlines that the GDPR leaves open. To complement the guide, the AEPD has also released a tool called 'Comunica-Brecha RGPD', which offers help to organisations in deciding whether or not to communicate a data breach to the affected individuals, a separate obligation to notifying the breach to the supervisory authority. This resource is based on a short form that, once completed, will advise three possible scenarios: (i) it is necessary to notify the security breach to the affected persons as a high risk is appreciated; (ii) no such communication is necessary; or (iii) or the level of risk cannot be determined. The final decision must be made by the controller based on the specific facts of the processing and circumstances of the breach.	25 May 2021	Guide on notification of personal data breaches (in Spanish). Tool 'Comunica-Brecha RGPD' (in Spanish).
New law on the protection of personal data processed for the	The Organic Law 7/2021, of May 26 is the transposition into Spanish law of Directive (EU) 2016/680 of 27 April 2016 on the	26 May 2021	Organic Law 7/2021, of May 26, on the protection

Development	Summary	Date	Links
prevention, detection, investigation and prosecution of crime	protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal penalties. The main purpose is to ensure that the data is processed by competent authorities in such a way as to fulfil the intended purposes, as well as to establish the highest standards of protection of the fundamental rights and freedoms of citizens. Among other issues: (i) a duty of collaboration with the competent authorities is included; (ii) the terms of conservation and review of the personal data processed are regulated; (iii) certain conditions are required that determine the lawfulness of any processing of personal data; (iv) the rights of individuals are established, indicating a series of general conditions for the exercise of rights (and establishing that these rights may be restricted for certain specified reasons); (v) the obligations and responsibilities of controllers and processors are determined; (vi) certain obligations are established that respond to a new model of active responsibility that requires a prior assessment of the risk that the processing of personal data could generate for the data subjects, in order to adopt the appropriate measures on the basis of this assessment; and (vii) transfers of personal data carried out by the competent Spanish authorities to a territory that is not a member of the EU or an international organisation are regulated. Finally, the specific sanctioning regime applicable to breaches of the obligations set forth in this Organic Law is regulated, and the subjects to be held liable for the infringements committed are defined.		of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions (in Spanish)
AEPD issues guide on risk management and data protection impact assessments	This guide has been published by the AEPD, with the aim of bringing together the experience accumulated in this field since the implementation of the GDPR, including the interpretations of the AEPD, the European Data Protection Board and the European Data Protection Supervisor. The document, aimed at controllers, processors and data protection officers, is applicable to any processing operation, regardless of its level of risk. In addition, and for cases of high-	29 June 2021	Guide on Risk management and impact assessment in the processing of personal data processing (in Spanish). Tool "Evalúa riesgo RGPD" (in Spanish).

Development	Summary	Date	Links
	risk processing, it incorporates the necessary guidelines for carrying out the data protection impact assessment (DPIA) and, where appropriate, the prior consultation referred to in Article 36 of the GDPR. The guide consists of three sections: (i) a description of the fundamentals of risk management for rights and freedoms; (ii) the basic methodological development for the implementation of risk management; and (iii) cases in which it is necessary to perform a PIA, with the necessary guidance to carry it out. In addition, the AEPD has presented "Evalúa_riesgo RGPD", the prototype of a new tool that helps controllers and processors to identify the risk factors for the rights and freedoms of data subjects present in the processing. The assessment of the level of risk for each factor carried out by the tool, as well as the final calculation of the level of risk, is of a general nature and represents a minimum assessment that, if necessary, will have to be adjusted by the controller to accurately determine the level of risk of the processing. Risk management and DPIAs are processes that are closely linked, since the latter is a specific part of the former. Thus, a DPIA cannot exist without being part of a risk management exercise, so while risk management is mandatory for all processing, the specific obligations established for DPIAs are exclusively for high-risk processing.		

Sweden

Contributors

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

Sina Amini
Associate
T: +46 7 24 51 25 34
sinaamini@
eversheds-sutherland.se

Development	Summary	Date	Links
Swedish DPA initiates audit of mutual fund advisor	The Swedish Authority for Privacy Protection (the "**Swedish DPA**") has initiated an audit of a Swedish company after receiving complaints about the company having incorrectly sent out personal data relating to several thousands of customers by e-mail.	16 April 2021	Press statement (in Swedish) Audit statement (in Swedish)
Swedish DPA releases previously published guidelines concerning data protection rights of children and young people on digital platforms in English	The Swedish DPA together with two other Swedish public authorities have released previously published guidelines concerning the data protection rights of children and young people on digital platforms (in English). The guidelines primarily aim to reach stakeholders who create and operate various digital environments where children and young people regularly spend time. The guidelines cover, amongst other things, under what circumstances consent is an appropriate legal basis for processing personal data relating to children and young people, use of geolocation data, connected toys and age verification.	28 April 2021	Press statement (in Swedish) Guidelines
Swedish DPA publishes guidelines concerning camera surveillance	The Swedish DPA has published guidelines concerning the use of camera surveillance. The guidelines are divided into two main sections. The first section covers general data protection requirements applicable for all uses of camera surveillance in Sweden and also includes a report on applications for camera surveillance permits between the period 1 August 2018 to 31 December 2020. The report concludes that the most common reason to request a permit for camera surveillance is to provide security for property and that the majority of these applications have been denied due to the applicant failing to provide sufficient	26 May 2021	Press statement (in Swedish) Guidelines (in Swedish)

Development	Summary	Date	Links
	documentation regarding relevant criminal activity on the company's premises. The second section provides guidance in more detail concerning the use of camera surveillance in specific areas such as schools, streets, healthcare facilities and parking lots.		
Stockholm administrative court rejects appeals from healthcare providers concerning fines imposed by the Swedish DPA	In December 2020 the Swedish DPA imposed administrative fines against eight healthcare providers for failing to limit access to the main system handling patient records. Five of these healthcare providers appealed the decision to Stockholm administrative court. Four of these appeals were rejected outright and the fifth resulted in the administrative fine being lowered. The court stated that the negligence of healthcare providers to conduct a risk assessment concerning the employees' access to patient records was in violation of GDPR.	28 May 2021	Press statement (in Swedish)
Swedish DPA concludes audit on personal data breach	The Swedish DPA has concluded its audit on a personal data breach by a healthcare services company. The audit was initiated when it was revealed that recorded phone calls to the company were available on the internet without password protection. The Swedish DPA imposed an administrative fine of SEK 12,000,000 against the controller as well as several smaller administrative fines ranging from SEK 250,000 to 650,000 against some of the involved processors which included three Swedish counties.	8 June 2021	Press statement (in Swedish)
Swedish DPA: Wrong to conduct around the clock camera surveillance in a fire station	The Swedish DPA has imposed an administrative fine of SEK 350,000 against a municipal association for conducting around the clock camera surveillance inside a fire station. The Swedish DPA stated that camera surveillance was only necessary when an alarm is sent to the fire station and that camera surveillance included sensitive areas such as the firefighters' locker room.	10 June 2021	Press statement (in Swedish) Decision (in Swedish)
Company fined SEK 16,000,000 by Swedish DPA for using body cameras	The company responsible for Stockholm's public transportation, which is owned by the Stockholm county, has been found to be in violation of GDPR by the Swedish DPA for using body cameras on their ticket controllers. The body cameras were continuously recording sound and video which was stored for one minute and	21 June 2021	Press statement (in Swedish) Decision (in Swedish)

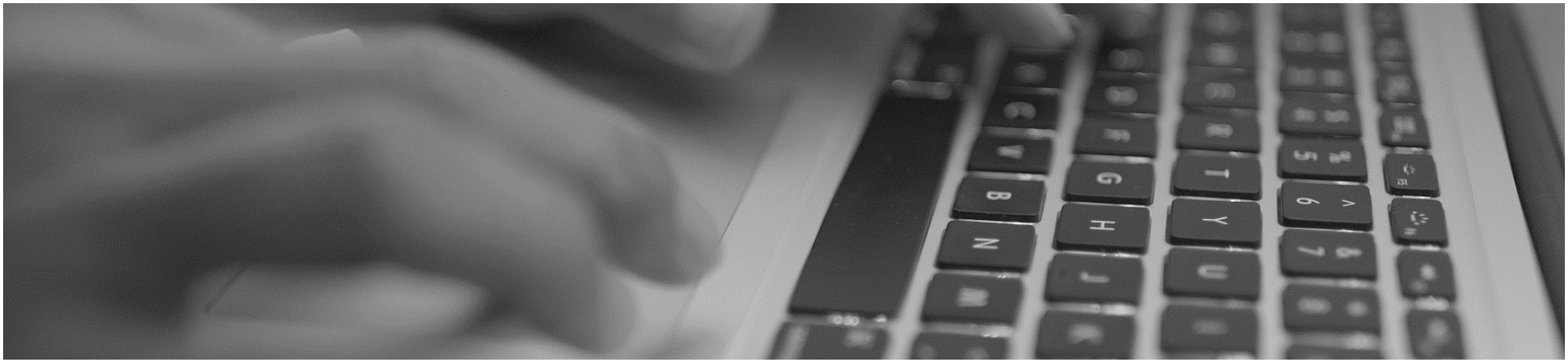
Development	Summary	Date	Links
	then deleted unless the ticket controller pressed the record button on the camera. The Swedish DPA stated that the fact that the ticket controllers were instructed to use the body camera during their work shifts meant that potentially any traveller could be recorded during ticket controls. The Swedish DPA also criticized the company for not informing travellers that the body cameras were also recording sound. An administrative fine of SEK 16,000,000 was imposed by the Swedish DPA.		
Swedish DPA publishes a report on personal data breaches notified to the Swedish DPA during 2020	The Swedish DPA has published a report on personal data breaches notified to the Swedish DPA during 2020. The report concludes that more than half of the notified personal data breaches were caused by human error. During 2020 approximately 4,600 personal data breaches were notified to the Swedish DPA.	22 June 2021	Press statement (in Swedish) Report (in Swedish)
Swedish DPA initiates audits on two Swedish companies for transferring personal data to Facebook	The Swedish DPA has received notifications of personal data breaches from two Swedish companies stating that personal data has been continuously transferred to Facebook for a longer period than agreed, due to incorrect settings. As a result of these notifications the Swedish DPA has initiated audits on the companies.	24 June 2021	Press statement (in Swedish)
Stockholm administrative court rejects appeal from a high school concerning administrative fine imposed by the Swedish DPA	In August 2019 the Swedish DPA imposed an administrative fine of SEK 200,000 against a high school for utilizing facial recognition technology in order to check the students' attendance. The high school appealed the decision made by the Swedish DPA to Stockholm administrative court. Stockholm administrative court rejected the appeal and stated that the high school has a right to check for the students' attendance but do not have the right to use biometric data for this purpose.	24 June 2021	Press statement (in Swedish)

Switzerland

Contributors

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

Development	Summary	Date	Links
Swiss Government publishes draft of the new Swiss Ordinance to the new Federal Act on Data Protection.	On 23 June 2021, the Swiss Federal Council has published the draft of the Ordinance to the new Federal Act on Data Protection. The new Federal Act on Data Protection was adopted on 25 September 2020, but has not yet entered into force (see Updata Edition 9). The draft of the Ordinance contains numerous implementation rules and concretisations of the new Federal Act on Data Protection, amongst others with regard to technical and organisational measures, cross-border data transfers and the rights of the data subjects. A consultation process is now in Progress until mid-October 2021. We anticipate therefore, that the new Federal Act on Data Protection and the new Ordinance will not enter into force before July 2022.	23 June 2021	



United Kingdom

Contributors

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

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

Development	Summary	Date	Links
Opinion on UK Adequacy decision	On 13 April 2021, the EDPB issued two separate Opinions in response to the European Commission's draft adequacy decision issued in February 2021. The two Opinions, Opinion 14/2021 and Opinion 15/2021 set out the EDPB's position in respect of the General Data Protection Regulation 2016/679 (GDPR) and the Law Enforcement Directive 2016/680 (LED) respectively. The EDPB primarily assessed the UK regime against the GDPR Adequacy Referential (adopted in 2018) and the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. On the whole, the EDPB noted that there was a strong alignment between the GDPR and the UK's legal framework. However, the EDPB also raised concerns over a list of potential challenges, including the fact that the UK Government had indicated its intention to develop separate and independent policies on data protection that could diverge from the EU's approach. Other challenges included, for example, the UK Data Protection Act's immigration exception and rules relating to onward transfer of personal data (i.e. where personal data is transferred from the EEA to the UK under the prospective adequacy decision and then further transferred from the UK onward to a third country).	13 April 2021	Opinion 14/2021 Opinion 15/2021
UK proposals for legislation on consumer smart product cybersecurity	In July 2020 the UK Government undertook a call for views on proposals to regulate consumer smart product cyber security. The Government has now published its response to this call. It intends to put in place legislation that will place obligations on economic actors to ensure that consumer smart products are only put on	21 April 2021	DCMS press release Response to call for views

Development	Summary	Date	Links
	the UK market if they comply with specific security standards (no universal default passwords, procedures in place to manage reports of security vulnerabilities and transparency on provision of security updates) and manufacturers will be required to publish a declaration of conformity in relation to the product, provide a public point of contact to make it easy to report vulnerabilities with the device and comply with enforcement measures. The Government plans to introduce the new law as soon as possible and has published two research reports with evidence supporting the new law.		
ICO position paper on the UK Government's proposal for a trusted digital identity system	The Information Commissioner's Office ("**ICO**") issued a position paper on the UK Government's proposal for a trusted digital identity framework. In February 2021, the UK Government issued a policy paper for the UK digital identity and attributes trust framework proposing that a new, trusted, digital identity system is established. In its position paper, the Commissioner welcomed the decentralised approach to the framework proposed by the Government and the data protection by design and default that the Government is pursuing. The ICO also highlighted relevant practical requirements of data protection law that must be implemented for the project. The position paper is a continuation of the ICO's engagement on this project having previously responded to the 2019 DCMS digital identity consultation. Separately the ICO had also engaged with the Scottish Government on the development of their Digital Identity Scotland programme.	22 April 2021	Blog ICO position paper (April 2021) Policy paper (February 2021)
Lloyd v Google – data protection lawsuit continues in the UK Supreme Court	The appeal in *Lloyd v Google* came before the UK Supreme Court at the end of April. In the case, Richard Lloyd, who fronts a campaign called Google You Owe Us, is seeking between £1.5 billion and £3 billion in compensation from Google on behalf of Safari users who had secret tracking cookies implanted on their devices from 2011 to 2012. The issue in dispute remains whether the Respondent (Lloyd) should have been refused permission to serve his representative claim against the appellant out of jurisdiction because: (i) the members of the class had not suffered "damage" within the	30 April 2021	Case details

Development	Summary	Date	Links
	meaning of section 13 of the Data Protection Act 1998 (DPA 1998); and/or (ii) the Respondent was not entitled to bring a representative claim because other members of the class did not have the 'same interests' in the claim and were not identifiable; and/or (iii) the Court should exercise its discretion to direct that the Respondent should not act as a representative. The ICO has intervened in the case, making representations to the Court on its position that loss of control of data should constitute 'damage': *"If loss of control does not constitute "damage" within the meaning of the DPA 2018, that may affect the commissioner's decisions as to whether and how to intervene in regulatory matters where there have been significant breaches of data protection law that have resulted in a loss of control for the affected data subjects but without there being evidence of material damage or distress."* The ICO argued that the right to control one's own personal data is an intrinsic right and that, just as with other fundamental rights, it is vital for society to ensure data protection. The case will have huge repercussions for the future of data protection litigation – for example, it could lead to a tariff being set for damages as a result of distress, if financial loss cannot be shown.		
ICO releases blog post on creating a new code of practice for the Journalism industry	On 7 May 2021, the ICO published a blog post regarding its work on creating a new code of practice for the journalism industry, which has recommenced after being paused due to the COVID-19 pandemic. In particular, the ICO highlights the importance of maintaining a good balance between freedom of expression and data protection law in the interests of democracy. The ICO states that it is updating its current guide for the media (published in 2014) and developing a new code of practice in line with its statutory requirement under section 124 of the Data Protection Act 2018.	7 May 2021	Blog ICO guide for the media (2014)

Development	Summary	Date	Links
	The guidance will be aimed at persons processing personal data for journalistic purposes, and will seek to clarify their legal obligations and how to comply effectively with these. The ICO will use feedback gathered during its call for views in April 2019 to help form the guidance. In addition, the ICO will issue a new public consultation this summer calling for further feedback.		
National Cyber Security Centre launches Early Warning notification service for cyber threats	On 11 May 2021, the National Cyber Security Centre announced it was providing a free online notification service (an Early Warning service) to organisations to inform them of threats against their networks. The system processes a number of UK-focused threat intelligence feeds from trusted public, commercial and closed sources, including several privileged feeds not available elsewhere. Once an organisation feeds in details of its assets, the Early Warning service will deliver feeds of (i) incident notifications – any activity that suggests an active compromise of a system, (ii) network abuse events – which indicate assets have been associated with malicious activity, and (iii) vulnerability alerts - indications of vulnerable services running on assets.	11 May 2021	Press release
Call for information on the Computer Misuse Act 1990	The Home Office published a call for information on the Computer Misuse Act 1990, which aims to identify whether there is activity causing harm in the area covered by the Act that is not adequately addressed by the offences set out in this 30 year old statute, as well as to collate other suggestions on how legislation could strengthen the response to cyber-dependent crime. The call for information closed on 8 June 2021.	12 May 2021	Press release
LIBE resolution recommending the European Commission amends draft UK adequacy decisions passed by European Parliament	On 15 May 2021 the Civil Liberties, Justice and Home Affairs Committee of the European Parliament ("**LIBE**") issued a nonbinding resolution which evaluated the Commission's approach on the adequacy of the UK's data protection regime. The resolution urges the Commission to amend the draft UK adequacy decisions in line with recent comments set out in the Opinions of the European Data Protection Board, primarily based on concerns surrounding:	15 May 2021	Press release Resolution EDPB Opinions

Development	Summary	Date	Links
	– UK bulk access practices and exemptions to data protection rights in cases of national security and immigration; and – onward transfers of EU citizens' data to third countries, for example, via the UK's data-sharing agreements with the US (especially concerns in light of the *Schrems II* judgment). The resolution, whilst non-binding, was passed on 21 May 2021 (with 344 votes in favour, 311 against and 28 abstaining) and applies additional pressure on the European Commission to reconsider its draft UK adequacy decisions. The European Commission may well amend its draft decision on UK data protection to ensure EU standards for citizens' privacy are respected. Many will be wondering if the European Commission will now adopt the UK adequacy decisions on time, that is before the end of the interim period, in order to avoid any disruptions for EU to UK data flows. It is anticipated that the Commission will make its decision on UK adequacy within the next few months. This is not welcome news to many in the UK who may well now have to look to EU/UK data transfer agreements containing standard contractual clauses, unless the bridge is extended past end of June. The ICO is yet to comment.		
Call for views on improving cyber security in supply chains	The UK Government issued a call for views on improving cyber security in supply chains and in managed service providers. This forms part of the Government's National Cyber Security Strategy 2016–2021. The aim is to assist businesses with an aspect of cyber resilience that many find challenging. This challenge is illustrated by the Cyber Security Breaches Survey 2021, which found that only 12% of businesses review cyber risks coming from immediate suppliers while only 5% address risks coming from wider supply chains. These vulnerabilities are growing as supply chains become increasingly interconnected. Part 1 of the call for views details: – barriers to effective supplier cyber risk management, such as low recognition of supplier risk, limited visibility into supply chains and inefficient expertise in spotting issues.	17 May 2021	Call for views National Cyber Security Strategy 2016-2021

Development	Summary	Date	Links
	– the principles for assisting in supply chain cyber risk management, such as understanding the risk and setting up control of supply chains. – supplier assurance - priority areas organisations should consider when ensuring their suppliers have appropriate cyber security protocols in place. – existing commercial offerings that can be used for management of supply chain cyber risk. – additional government support that is available. Part 2 details: – the pros and cons of managed service providers. – the principles of the existing Cyber Assessment Framework, and seeking views on whether this should apply to managed service providers. – preliminary policy options that effectively promote the use of managed service provider security standards (e.g. by establishing certification or assurance marks). The call for views closed on 11 July 2021.		
Data Sharing Code of Practice is laid before Parliament	The Data Sharing Code of Practice was laid before Parliament by the UK Government on 18 May 2021. The Code will lay before Parliament for 40 sitting days before coming into force. The code, a statutory code of practice made under section 121 of the Data Protection Act 2018, is available in full on the ICO's website; many organisations will be familiar with it and will have been adhering to it (given it shows what the regulator expects) ever since it was published last year. The ICO says in it that those who do not follow it may find it much more difficult to comply with the accountability principle of UK GDPR (which is why it has been taken on board by many already). It sets out key information on what should be included in data sharing agreements (for example, contracts will need to include the purpose of data sharing, what data items will be shared, the lawful basis for sharing the data and permitted uses by each party), as well as other considerations around the provision of	18 May 2021	Data sharing: a code of practice ICO statement

Development	Summary	Date	Links
	personal data from one controller to another and as between joint controllers. According to the ICO, the aim of the code is "*to give businesses and organisations the confidence to share data in a fair, safe and transparent way, and it dispels many of the remaining myths about data sharing. The code will guide organisations through the practical steps they need to take to share data while protecting people's privacy.*"		
Court of Appeal holds DPA 2018 "immigration exemption" incompatible with GDPR	The Court of Appeal has issued its judgment in the case of *The Open Rights Group & Anor, R (On the Application Of) v The Secretary of State for the Home Department & Anor [2021] EWCA Civ 800*. The case relates to the lawfulness of the "immigration exemption" under Schedule 2 paragraph 4 of the Data Protection Act 2018 (the "**DPA 2018**"), which allows certain aspects of the DPA 2018 to be disapplied if their application is likely to prejudice immigration control. The appellants argued that the immigration exemption is incompatible with Article 23 of the GDPR, the provision authorising this type of exemption, and/or incompatible with Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union (the "**Charter**"). The Court of Appeal held that the immigration exemption is incompatible with Article 23 of the GDPR, and the appeal was allowed. In light of this, the Court found it unnecessary to address the appellants' additional contention regarding incompatibility with the Charter. The Court of Appeal deferred its decision on relief, and invited further submissions on the appropriate remedy. The judgment has been welcomed as part of the UK's efforts to secure an adequacy decision enabling personal data to flow freely from the EU to the UK.	26 May 2021	Judgment

Development	Summary	Date	Links
ICO calls for views on first chapter of draft anonymisation, pseudonymisation and privacy enhancing technologies guidance	On 28 May 2021, the ICO issued a call for views on the first chapter of its draft guidance on Anonymisation, pseudonymisation and privacy enhancing technologies. The first chapter, "Introduction to anonymisation", explores issues surrounding anonymisation and pseudonymisation from a data protection law angle (e.g. when personal data can be considered to be anonymised; whether it is possible to anonymise data adequately to reduce risks; the potential benefits of anonymisation and pseudonymisation). Further draft chapters will be published this summer and autumn. Views should be submitted to anonymisation@ico.org.uk. The consultation on the first draft chapter will close on 28 November 2021.	1 June 2021	Press release Draft chapter
Research into cyber security sector	The UK Government is carrying out research to understand the UK cyber security sector and how it is growing in order to inform policy in this area. Participants in the UK cyber security sector have been selected and will be contacted by Ipsos MORI.	1 June 2021	Press release
Research into business use of connected devices and cyber security risk	The UK Government is carrying out research into how UK businesses procure, use and manage connected devices within their networks in the context of cyber security risk awareness and management. Telephone interviews will take place in June and July.	2 June 2021	Statement
NCSC outlines what board members should know about ransomware, and what they should ask their technical experts	A blog post published by the National Cyber Security Centre sets out why board members should concern themselves with ransomware, what board members need to know about ransomware, and what board members should ask their technical experts about ransomware. The blog reminds board members that cyber security within a company is the responsibility of the board, and that ransomware attacks targeted at companies are increasing in frequency. The blog addresses five specific questions for board members to ask their technical experts, namely: – How would we know when a ransomware incident occurred?	3 June 2021	Blog

Development	Summary	Date	Links
	– What measures should the organisation take to minimise damage to our network caused by a ransomware attack? – Does the organisation have an incident management plan for cyber-attacks; how do we ensure that the plan is effective? – Does our incident management plan meet challenges posed by ransomware incidents? – How is our data backed up? Would backups be unaffected by a ransomware attack?		
NCSC provide updates to its alert on ransomware incidents affecting the UK education sector following further attacks on the sector by cyber criminals	In light of a further increase in ransomware attacks against establishments in the UK education sector, on 4 June 2021, the National Cyber Security Centre published an updated version of its alert regarding ransomware attacks on the UK education sector by cyber criminals. The updated alert lists further trends seen in ransomware attacks on the UK education sector, as well as providing mitigation advice to help protect UK education establishments from being targeted by cyber criminals.	7 June 2021	Press release Alert
CMA response to call for information on harms to competition and consumers caused by algorithms	In January 2021, the Competition and Markets Authority ("**CMA**") published a paper "Algorithms: How they can reduce competition and harm consumers" which explored how algorithms can be used to harm consumers including by way of personalisation of pricing and other consumer choices, exclusion of competitors and collusion. In addition, the paper summarised the techniques that can be used to analyse algorithmic systems and the role of regulators in addressing the risk involved in their use. The CMA also launched a consultation regarding the paper, which closed on 16 March 2021. A summary of the responses received has been published. The CMA plans to use the responses to inform and enhance its analysing algorithms programme.	18 June 2021	Responses to consultation Consultation page Original report (19 January 2021)
Taskforce on Innovation, Growth and Regulatory Reform recommends replacing GDPR	The Taskforce on Innovation, Growth and Regulatory Reform has issued a report in response to its objective to "*look at ways to refresh the UK's approach to regulation now that we have left the EU, and to seek out opportunities to take advantage of our new-found regulatory freedom, to support innovation and growth*".	16 June 2021	Details of Report Report

Development	Summary	Date	Links
	The report calls for the UK to replace its existing data protection regime (based on the EU GDPR) with "*a new, more proportionate, UK Framework of Citizen Data Rights to give people greater control of their data while allowing data to flow more freely and drive growth across healthcare, public services and the digital economy*". The taskforce's proposals include: – creating a new regulatory infrastructure and exploring the possibility of establishing "data trusts" or "data fiduciaries" in order to give people meaningful control of their data; and – removing Article 22 GDPR to permit automated decision-making for machine learning and harness the potential of artificial intelligence. It will be interesting to observe how the role this report has in shaping the UK Government's policy as regards data protection law, and how that may affect the UK's recent finding of adequacy for data transfers from the EU.		
ICO report on use of facial recognition	The ICO has written about the use of live facial recognition technology ("**LFR**") in a new report and accompanying blog post. The ICO outlines what LFR is, the data protection issues involved and the steps being taken to investigate and advise on its use (including assessing DPIAs, conducting audits and supporting codes of conduct and certification schemes). The report sets out a number of "key requirements" for controllers deploying LFR, and recommendations for industry to help build and maintain public confidence in the use of LFR.	18 June 2021	Blog Opinion
European Commission adopts UK adequacy decisions	The European Commission has adopted two adequacy decisions covering transfers of personal data from the EU to the UK – one agreement under the GDPR and another under the Law Enforcement Directive. Read our full client briefing here. This means that the UK is recognised formally as providing an "essentially equivalent of protection" to personal data flowing from the EU. Therefore, organisations may facilitate transfers	28 June 2021	Eversheds Sutherland briefing Press statement

Development	Summary	Date	Links
	from the EU to the UK without the need for specific transfer tools and supplementary measures. The agreements reference the UK's data protection legal rules which continue to be based on the GDPR and Law Enforcement Directive, and the UK being subject to the jurisdiction of the European Court of Human Rights, as key factors in support of the adequacy findings. Therefore, there is somewhat of a shadow over the longevity of the agreements, due to the TIGGR proposals for a new UK data protection framework, and the UK Government's review of the Human Rights Act 1998 by an independent expert panel. As a counterbalance to those concerns, it is worth recalling that an adequacy decision was recognised by the UK Government as a key element in the exit arrangements with the EU, and has been strongly lobbied for, in the past six months because of its importance to trade and growth. It is a precious prize, hard won. So for now, some good news for UK trade, as well as for those many international organisations battling to deal with the myriad of data protection law changes. The agreements also contain a sunset clause which limits the duration of their validity to four years after their entry into force. During these four years, the Commission will monitor legal developments in the UK and can intervene to review the adequacy finding at any point if the UK's privacy protections are deviated from. The GDPR adequacy finding excludes transfers for the purposes of UK immigration control to reflect the recent Court of Appeal judgment.		

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

Pooja Kohli
Associate
T: +1.212.389.5037
pkohli@
eversheds-sutherland.com

Development	Summary	Date	Links
The Federal Trade Commission (FTC) emphasis the need for corporate boards to prioritize data security	On 28 April 2021, the Federal Trade Commission (FTC) issued guidance and recommendations to corporate boards to make sure data security gets the attention it deserves, particularly in light of recent settlements following challenges to allegedly deceptive or unfair conduct related to companies' data security practices. The FTC recommendations include: making data security a priority by setting the tone from the top and instilling a culture of security; tailoring security programs to a company's unique needs, priorities, technology, and data; responding effectively to security incidents; and learning from the company's mistakes as well the mistakes of others.	28 April 2021	FTC guidance
Proposed Amendments to New York Privacy Law	On 12 May 2021 New York Bill S.6701 (the New York Privacy Act) was introduced into the New York State Senate. The bill (amongst other things) proposes that controllers have a duty of loyalty to consumers; prohibits unfair, deceptive or abusive acts with respect to obtaining consent, processing of data and consumer	12 May 2021	New York Bill S.6701

Development	Summary	Date	Links
	rights; requires businesses to conduct risk assessments; requires businesses to disclose their methods of de-identifying personal information, to place special safeguards around data sharing; and to allow consumers to obtain the names of all entities with whom their information is shared. If passed in its current form, the law would apply to legal persons who conduct business in New York or produce products or services that are targeted to residents of New York if one or more certain threshold requirements are met. It would not apply to information collected, processed, disclosed or sold pursuant to the Gramm-Leach Bliley Act. The legislature expects to work on the bill over the summer as a high priority.		
Amendments to Connecticut and Texas Data Privacy Laws	On 16 June 2021, Connecticut's Data Privacy Breach Law was amended to expand the definition of "personal information" and reduce the timescale for providing notification of a data breach affecting a Connecticut resident from ninety days to sixty days. On 14 June 2021, Texas' Breach Notification Law was amended to require the state Attorney General (AG) to name and shame by posting notice of data breaches on a public website within 30 days of receiving notification of that breach. The amendments also require the companies to provide the AG with the number of affected residents notified of the breach in addition to existing notification requirements.	Amendment to Connecticut Data Privacy Breach Law: 25 June 2021 Amendment to Texas Breach Notification Law: 14 June 2021	Connecticut law Texas law
2021 Colorado Privacy Act Passes	On 25 June 2021, Colorado sent Senate Bill 21-190 (the Protect Personal Data Privacy Act) to the Governor for signature. The bill is expected to be signed into law imminently and will provide enhanced disclosure obligations on companies and provide enhanced rights to Colorado consumers, including the right of access, deletion, rectification and to opt out of the sale, collection or use of data.	25 June 2021	Colorado 2021 Privacy Bill

For further information, please contact:

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

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

@ESPrivacyLaw

Editorial team

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

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

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

Eleanor Gill
Trainee Solicitor
M: +44 791 751 6738
eleanorgill@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