EVERSHEDS SUTHERLAND

Updata

Your quarterly Data Privacy and Cybersecurity update

July to September 2021

Executive summary

Welcome to the latest edition of Updata!

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

This edition covers **July to September 2021** and is full of newsworthy items from our team members around the globe, including updates along the following themes:

- The use of cookies is increasingly coming under scrutiny, including court cases filed in Austria, as well as developments in the UK, France, Italy and a cookies taskforce being set up at EU level
- Regulatory enforcement continues to intensify against both small and large companies, including in California
- The privacy implications of artificial intelligence are also increasingly the subject of regulatory activity, including in Singapore and the UK
- The proliferation and evolution of global privacy regulations continues, with Saudi Arabia enacting its first comprehensive data protection law, the UK DCMS' proposals to overhaul the data protection legal regime, and China's finalisation of its Personal Data Protection Law, which goes into effect on 1 November
- Cross border restrictions continue to evolve, with China setting out new provisions for overseas transfers of personal data (including from connected vehicles),and with the UK ICO's consultation for transfers of personal data out of the UK and in the UK

We hope you enjoy this edition of Updata.

Follow us on Twitter at:

@ESPrivacyLaw

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

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

General EU and International

Contributors

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

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

Development	Summary	Date	Links
European Parliament adopts temporary exemption to ePrivacy Directive to detect child sexual abuse online	Members of the European Parliament ("**MEPs**") authorised a temporary regulation allowing web-based service providers to continue fighting child sexual abuse material online on a voluntary basis. The MEPs backed the new legislation in a move to more effectively protect children from sexual abuse and mistreatment online, which has been further exacerbated by the COVID-19 pandemic. The agreement on the new temporary legislation anticipates a temporary derogation from certain Directive 2002/58/EC provisions, including Article 5(1) which concerns the confidentiality of communications online, and Article 6(1) which concerns traffic data online is expected. The Regulation was published in the Official Journal on 30 July 2021 and came into force on 2 August 2021. The new legislation will apply for a maximum of three years (or fewer if new permanent rules on tackling child sexual abuse online are agreed in the meantime).	6 July 2021	Regulation final text
EDPB adopts guidelines 07/2020 on the concepts of controller and processor	The European Data Protection Board ("**EDPB**") published the final version of its Guidelines 07/2020 on the concepts of controller and processor in the GDPR. The detailed guidelines clarify the concepts of controller, joint controller and processor, as well as explaining the roles and the distribution of responsibilities between the parties, based on the definitions in Article 4 of the EU GDPR and the provisions on obligations in Chapter IV of the EU GDPR.	7 July 2021	Guidelines 07/2020

Development	Summary	Date	Links
	In brief, the guidelines say that: – a controller is a body that decides upon the purposes and means of the processing, i.e., it determines the why and the how of the processing. There is no requirement for a controller to have access to the data to be classed as a controller; – joint controllership exists when two or more entities participate in the determination of the purposes and means of the processing. Decisions can be made by common decision (i.e., the controllers decide together) or can result from converging decisions (i.e., the decisions complement each other). For joint controllership to apply, it is important to note that the processing by each party must be inseparable; and – a processor is a natural or legal person that processes personal data on behalf of the controller. The processor entity must be separate from the controller, and must not process the data in a way that goes beyond the controller's instructions. If the processor does go beyond instructions given by the controller in relation to how the data should be processed, it risks falling into the definition of 'controller'. The guidelines also clarify the respective responsibilities of controllers, joint controllers and processors. EDPB guidance remains relevant to UK based companies that are subject to the EU GDPR (for example, because they have an establishment in the EEA, and/or provide goods/services or monitor the behaviour of EEA based individuals).		
EDPB adopts guidelines 04/2021 on codes of conduct as a tool for transfers of data	The EDPB published its guidelines on codes of conduct as tools for transfers of data. The guidelines aim to clarify the application of article 40(3) of the GDPR, which relates to the ability for codes of conduct to be used as appropriate safeguards for transfers of personal data to countries that are outside of the EU in accordance with article 46(2)(e) of the GDPR. The guidelines also contain practical support covering the content of codes of conduct, how codes of conduct are adopted and the	7 July 2021	Guidelines 04/2021 Guidelines 1/2019 on codes of conduct and monitoring bodies under Regulation 2016/679

Development	Summary	Date	Links
	stakeholders involved, along with the key requirements to be met by, and guarantees that need to be contained in, a code of conduct for transfers. The guidelines should be read in conjunction with the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, which set out a framework for adopting codes of conduct.		
EDPB adopts guidelines 02/2021 on virtual voice assistants	Following public consultation, the EDPB issued its updated Guidelines 02/2021 on virtual voice assistants ("**VVA**") that understand voice commands and execute them or mediate with other IT systems, such as those available on smart devices (eg, computers, smartphones, tablets, smart TVs or smart speakers). The guidelines highlight that VVAs process huge amounts of personal data. They seek to assist stakeholders to address compliance issues under the EU GDPR and the EU e-Privacy Directive when providing VVA services, by identifying some of the most relevant privacy and cyber security challenges and suggesting how these can be addressed. The guidelines focus on four common areas where VVAs process personal data, namely: executing requests; improving the VVA machine learning model; biometric identification; and profiling for personalised content or advertising. Special consideration has been given to the processing of children's data. The guidelines cover recommendations and advice in relation to the provision of the mandatory transparency information; a separate registration for each VVA functionality; the choice of lawful basis for the processing of personal data; data retention periods; access control mechanisms; the need to filter out background noise to protect privacy; the requirement to undertake a Data Protection Impact Assessment; and facilitation of the exercise of data subject rights through the use of simple voice commands.	7 July 2021	Guidelines 02/2021
EDPB consults on guidelines on codes of conduct as tools for transfers	The EDPB launched a consultation on new guidelines on codes of conduct as tools for transfers. The guidelines, initially published on 7 July 2021, work alongside the EDPB's guidelines on codes of conduct and monitoring bodies. The consultation ran until 1	14 July 2021	Guidelines for consultation

Development	Summary	Date	Links
	October 2021. The guidelines aim to specify the application of Article 40(3) of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries. They also aim to provide practical guidance including on the content of such codes of conduct, their adoption process and the actors involved as well as the requirements to be met and guarantees to be provided by a code of conduct for transfers.		
EDPS discusses synthetic data and data protection in blog post	On 14 July 2021, the EDPS published a blog post on synthetic data and data protection. Synthetic data is defined by the OECD as *"An approach to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released."* Synthetic data allows the retention of the original statistical properties while potentially adding an additional layer of protection. However, the debate is still open on whether synthetic data confers meaningful privacy benefits. The blog post discusses a recent EDPS IPEN webinar, held on 17 June 2021, titled *"Synthetic data: what use cases as a privacy enhancing technology?".* During the webinar, experts were divided on the practicality and usefulness of synthetic data as compared to traditional forms of data anonymisation.	14 July 2021	EDPS blog post
European Parliament committee adopts position on proposed Data Governance Act	The Industry, Research and Energy Committee of MEPs adopted rules to facilitate making more data available to help create new products and innovation, in particular in AI.	16 July 2021	Press release
ENISA report highlights growing cyber threats to supply chains	On 29 July, the European Union Agency for Cybersecurity ("**ENISA**") published a report examining the threat landscape of attacks on supply chains. The report explores what a supply chain attack is, explains the lifecycle of such an attack, highlights recent examples of supply chain attacks, analyses supply chain incidents, addresses the problem of misclassification of incidents as supply chain attacks	29 July 2021	Press release Report

Development	Summary	Date	Links
	and provides several high-level and technical recommendations aimed at customers and suppliers. Interestingly, the report highlights that attackers are increasingly targeting suppliers rather than customers. According to the report, this might be because customers have strengthened their security protection to combat attacks, and also because attackers can affect multiple customers using a supplier's product through targeting that supplier. The report estimates that supply chain attacks could increase fourfold in 2021 compared with 2020. 62% of the 24 incidents analysed in creating the report used malware in order to carry out their attack. In 66% of the incidents, the attackers' focus was on the suppliers' code. Around 58% of attacks focussed mainly on compromising customer data. In 66% of the incidents, suppliers were unaware of how the attack occurred, or failed to report how they were compromised; this contrasts with attacks on customers, where only 9% of those attacked were unable to say how the attacks occurred. The report concludes that it is vital that the EU applies good practice and establishes coordinated actions across member states in order to help reach a common level of security across the EU. The report also recommends that customers and suppliers take action to combat the threat of supply chain attacks.		
EDPB reports on data protection authorities' resources	The EDPB published a report in response to a request from the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament to share data protection statistics. LIBE was specifically concerned with the level of resources provided by Member States to their data protection authorities. The report therefore provides breakdowns of each data protection authority and other relevant metrics including employee numbers and enforcement case figures.	12 August 2021	Report
EDPS opinion on European Commission's consumer credit directive proposals	The European Commission adopted a proposal to replace Directive 2008/48EC on credit agreements for consumers as well as adapting the current rules to the continuing digitalisation of the market and other trends. The European Data Protection Supervisor ("**EDPS**") welcomed the aim of strengthening	26 August 2021	EDPS press release

Development	Summary	Date	Links
	consumer protection and recalled the complementary relationship between consumer and data protection.		
European Commission consults on protecting the rights of young people and children	The European Commission opened a consultation into protecting the rights of young people and children when they go online. This forms part of wider consultation activities aimed at creating a digital world where everyone can benefit from the opportunities being digital provides whilst also being fit for the future, as part of the EU's focus on digital transformation by 2030. The consultation closed on 11 October 2021.	1 September 2021	Consultation Consultation survey BIK strategy
ISO publishes new standard for cybersecurity in cars	The International Standard of Organisation ("**ISO**"), an independent, non-governmental internal organisation, has released a new standard for cybersecurity engineering for cars. The new standard, *ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering*, addresses the cybersecurity issues in the engineering of electrical and electronic systems within road vehicles and aims to enable organisations to define cybersecurity policies and processed, manage cybersecurity risk and foster a cybersecurity culture.	31 August 2021	Press release
European Commission's approach to IOT cybersecurity scrutinised by DigitalEurope	DigitalEurope released a new study on cybersecurity of the Internet of Things ("**IOT**"), finding that the European Commission's approach to cybersecurity leads to security risks in connection devices as well as legal uncertainty. The study entailed interviews with 18 standard experts, who identified a number of vulnerabilities within connected devices and suggested recommendations for how EU product legislation and harmonised standards should work together in an effort to uphold cybersecurity of connected products. DigitalEurope recommended that the European Commission 'prioritise new horizonal cybersecurity legislation applicable across all connected products' and that it should set a 'realistic timeframe for standards organisations to develop the necessary harmonised standards, thus maximising the link between legislation and standards'.	9 September 2021	DigitalEurope study

Development	Summary	Date	Links
Office of the High Commissioner for Human Rights releases statement on the use of artificial intelligence systems	The Office of the High Commissioner for Human Rights ("**OCHR**") released a report on the widespread use by nation states and business of AI, which – while acknowledging that such technologies can be positive and help societies overcome key challenges – focussed on how AI can impact an individual's enjoyment of the right to privacy, alongside other human rights. Among other recommendations, the OCHR emphasised the need for a moratorium on the sale and use of artificial intelligence ("**AI**") systems which pose a serious risk to human rights, until adequate safeguards are put in place. She also called for a ban of AI applications which are not compliant with international human rights law.	15 September 2021	Office of the High Commissioner for Human Rights press release Office of the High Commissioner for Human Rights report
EDPB 55th plenary leads to establishment of cookie banner taskforce and opinion on draft South Korea adequacy decision	At its 55th plenary, the EDPB discussed and adopted an opinion on the European Commission's draft adequacy decision for South Korea. In this opinion the EDPB considered that the main elements of the data protection framework in place in South Korea aligned to the essence of the fundamental data protection principles in place in the rest of the EU but has requested clarification and ongoing monitoring on the following points: – further detail on the enforceability, binding nature and validity of the administrative rule which sets out how the statutory text applies (Notification No 2021-1); – how effective remedies and redress will be implemented – pseudonymisation (in particular the effects on the fundamental rights and freedoms of data subjects whose personal data is transferred to South Korea); – withdrawal of consent (which under South Korean law only exists in specified circumstances rather than a general right to withdraw consent). The EDPB also established a cookie banner taskforce (under Article 70(1)(u) GDPR) with the purpose of responding to the complaints filed by the not for profit organisation NOYB. The taskforce will focus on exchanging views for legal analysis;	27 September 2021	55th EDPB Agenda Press release (Cookie banner taskforce) Press release (South Korea adequacy)

Development	Summary	Date	Links
	supporting activities at national level and coordinating consistent communication.		

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

Development	Summary	Date	Links
Supreme Court requests preliminary ruling from CJEU on lawfulness of data processing by social media platform	In the long-standing court case of the Austrian privacy activist Max Schrems against a global social media platform over alleged GDPR violations, the Austrian Supreme Court has referred parts of the matter to the Court of Justice of the European Union ("**CJEU**") requesting a preliminary ruling. The Supreme Court requested a ruling on the following matters: – is the social media platform's practice to base large parts of its processing activities on the legal basis of Article 6(1)(b) GDPR (necessity for the performance of a contract) compliant with the GDPR, or would the social media platform have to rely on consent (Article 6(1)(a) GPDR)? – is the principle of data minimisation (Article 5(1)(c) GDPR) violated if data held by the social media platform may be aggregated, analysed, and processed for the purposes of targeted advertising without any restriction on the nature of the data or the time it can be held for? – is Article 9 GDPR (restrictions on the processing of special categories of data) applicable if the special categories of data (eg political opinions or details of sexual orientation) can be filtered from the collected data for advertising purposes, even if the controller does not differentiate between this data?	Date of Decision: 23 June 2021 Published: 20 July 2021	Link to Decision (German) Machine translation of the decision into English, provided by the NGO noyb Statement by Max Schrems/noyb on the referral (English)

Development	Summary	Date	Links
	– is the Article 5(1)(b) GDPR (principle of purpose limitation) in conjunction with Article 9(2)(e) of the GDPR to be interpreted as meaning that a statement about one's sexual orientation for the purposes of a panel discussion permits the processing of other data on this data subject's sexual orientation for the purposes of aggregating and analysing data for personalised advertising? The CJEU's ruling on these matters will have a significant impact on the processing of personal data by both social media platforms and online advertisers in general.		
Supreme Court awards Max Schrems EUR 500 compensation over handling of DSAR and rules on household exemption, the roles of "controller" and "processor" and the required response to a DSAR	While some major questions in the court case of the Austrian privacy activist Max Schrems against a global social media platform over alleged GDPR violations were referred to the ECJ (see above), the Austrian Supreme Court has issued a final ruling on other questions in the case. The Supreme Court ruled that Max Schrems has a right to compensation of EUR 500 under Article 82 GDPR for the "massive annoyance" caused by the social media platform, particularly in relation to its incomplete response to Max Schrems' data subject access request ("**DSAR**") under Article 15 GDPR. The Supreme Court also ruled on the following matters: – that the processing of personal data on Max Schrems' social media profile, which was set to "private" and was therefore not publicly available, is covered by the "household exemption" (Article 2(2)(c) GDPR) and therefore not subject to GDPR; – that a social media platform user is not the controller of the data processing on their own private social media profile and subsequently, the platform is not a data processor, but rather a controller of this data; and – that it is not a sufficient response to a DSAR to provide access merely to the personal data that the controller deems "relevant". This is not changed by the fact that the other data may be accessed via an online tool. The Court stated that a DSAR should not be an "easter egg hunt" for the data subject. Furthermore, nine access requests during a period of	Date of Decision: 23 June 2021 Published: 20 July 2021	Link to Decision (German) Machine translation of the decision into English, provided by the NGO noyb Statement by Max Schrems/noyb on the decision (English)

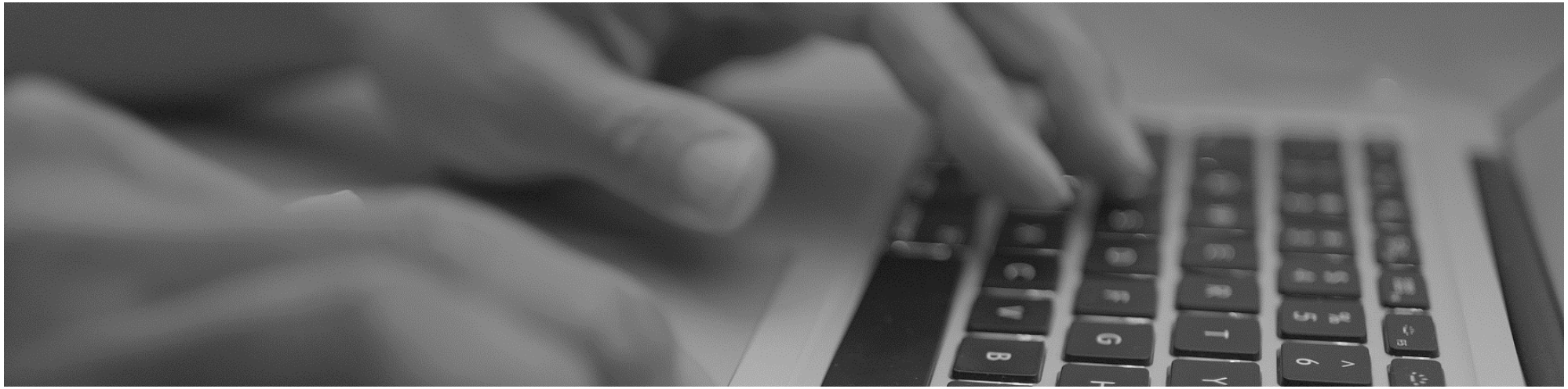
Development	Summary	Date	Links
	five years was not considered "excessive" within the meaning of Article 12(5) GDPR.		
Austrian DPA issues EUR 2 million penalty against loyalty program for unlawful profiling practices	The Austrian Data Protection Authority ("**DPA**") issued a fine of EUR 2 million against an Austrian loyalty program for unlawful profiling practices. The Austrian DPA found it was not sufficiently clear for customers signing up to the loyalty program that they were also consenting to the use of their personal data for profiling purposes. Following the first proceeding in relation to this, the loyalty program made this information clearer for new customers. The DPA claimed however that they did not stop using the affected data subjects' personal data for profiling, which led to the DPA imposing the fine. The personal data of approximately 2.3 million data subjects was affected. The loyalty program plans to appeal against the decision. Therefore, the decision is not yet binding.	2 August 2021	News report (German)
Austrian DPA rules that oil company's screening of employee work phones and emails violated GDPR	The Austrian DPA ruled that a major Austrian oil company violated data protection laws by reviewing their employees' professional phone records and email accounts without the consent of the company's Works Council. It is not known if the DPA has issued a fine or not. According to a news report, the company required their employees to consent to the company reviewing abbreviated itemized bills (with the last three digits deleted) from company cell phones as well as e-mails sent and received via the company e-mail account over a certain period of time. The company intended to match this data with certain target phone numbers and to screen for selected search terms to identify breaches of the employment contracts or of the applicable laws. The report claims that the Works Council was not involved in this screening. According to the report, the DPA issued a ruling declaring these screening measures to have been unlawful despite the employees' consent. The ruling has not yet been published. The company claims that all measures have been lawful and	6 August 2021	Report on news portal "Dossier" (German)

Development	Summary	Date	Links
	announced its plans to appeal against the decision. Therefore, the decision is not yet binding.		
NGO noyb issues complaints regarding cookie banners	The Austrian NGO noyb, founded by Max Schrems, filed 422 formal GDPR complaints against website operators for alleged unlawful use of cookie banners. Earlier this year, noyb sent letters to around 500 websites informing them of the NGO's intention to file a complaint unless the claimed violations of GDPR were remedied. While the NGO claims that many violations were actually remedied, most websites did not render their cookie banners fully compliant. Therefore, in August, the NGO filed 422 formal GDPR complaints against the responsible website operators. Approximately half of these complaints were filed at the Austrian DPA. The NGO identified the following issues as being most prevalent: – no option to reject cookies on first layer of the banner; – pre-ticked consent boxes; – link instead of button to exercise reject cookies option; – deceptive button contrast/colour; – unlawful use of legitimate interest; – marking cookies as essential that are not essential; and – withdrawing consent to cookies is not as easy as giving consent. The NGO expects the first decisions on their complaints around the end of this year. The EDPB has set up a taskforce to coordinate the response to these complaints.	10 August 2021	Link to report by noyb (English) Link to statement by EDPB (English)
NGO noyb issues complaints regarding "pay-or-okay" cookie walls	The Austrian NGO noyb filed complaints against seven major German and Austrian news websites for their use of cookie paywalls. The NGO claims that consent to the use of cookies on these websites was not freely given as the price for the use of the	13 August 2021	Link to report by noyb (English)

Development	Summary	Date	Links
	website without cookies was usually 10-100 times higher than the market price of the data otherwise collected. In 2019, the Austrian Data Protection Authority ruled that an Austrian news website's cookie paywall did not violate GDPR. However, noyb claims that this ruling was based on largely inaccurate information. Therefore, noyb hopes to reverse this ruling. The complaints were filed with Austrian and German DPAs.		
Federal Administrative Court asks CJEU to issue a preliminary ruling on Article 15(3) GDPR	The Austrian Federal Administrative Court (BVwG) is to decide on an appeal against a decision by the Austrian DPA. The proceeding was initiated by a complaint from a data subject who had filed a DSAR pursuant to Article 15 GDPR to a credit agency. Amongst other things, the complainant requested a copy of their personal data processed by the credit agency. In response to this request for a copy, the agency only provided a table that contained the personal data of the complainant in aggregated form but refused to provide a database print-out or copies of email correspondence regarding the complainant. The agency argued that Article 15(3) GDPR does not entitle a data subject to receive a fascimile copy of the data and that disclosure of a copy would also violate the agency's business secrets. The Austrian DPA agreed with the arguments of the credit agency and dismissed the complaint. The respondent appealed against this decision. The Austrian Federal Administrative Court stayed the proceeding and filed a request for a preliminary ruling from the CJEU on the interpretation and extent of the right to receive a copy under Article 15(3) GDPR. Amongst other questions, the Court asked whether the term "copy" is to be interpreted as meaning a photocopy/facsimile copy of the data, or if the term is to be interpreted as meaning a "transcript" of the data.	9 August 2021	Link to report on GDPR hub (English)
Supreme Court rules that credit agency's processing of 3 year old personal data relating to unpaid invoices did not violate GDPR	The Austrian Supreme Court decided on a case in which a claimant was requesting a credit agency to delete data about the claimant relating to information on a series of invoices that had not been paid by the claimant in 2017 and 2018. The claimant claimed that all unpaid invoiced had since been paid and that the	Date of Decision: 9 August 2021 Published: 19 August 2021	Decision (German) Summary of decision on GDPRhub (English)

Development	Summary	Date	Links
	claimant's financial situation had improved. Therefore, the claimant requested deletion of this data based on the right to be forgotten (Article 17 GDPR). The Supreme Court rejected the request for deletion of the data, ruling that the credit agency could base the processing on legitimate interest. In this context, the legitimate interest of the credit agency's customers in receiving a complete picture of the data subject's creditworthiness and payment behaviour had to be taken into account. In this context, the processing of this data for approximately only 3 years (at the date of the decision) was permissible. Furthermore, the Supreme Court stated (obiter dictum) that even the storage period of 10 years intended by the credit agency would have been permissible in this context.		
Austrian DPA requires credit agency to explain the logic behind calculation of credit scores	The Austrian NGO noyb filed a complaint in the name of a data subject against a credit agency. The data subject had been denied an energy contract due to their low creditworthiness. When the data subject filed a data access request to the credit agency, the agency claimed not to process any personal data about the data subject. The agency refused to explain how the data subject's credit score had been calculated, claiming that such explanation would violate trade secrets. It transpired that the data subject's credit score was calculated based only on the data subject's name, address, sex and date of birth, combined with demographic data. The Austrian DPA ruled that the agency was obliged to inform its customers about the fact that the calculation of their credit score was based only on their name, address, sex and date of birth, combined with demographic data and was not based on any data on payment behaviour of this particular data subject. Furthermore, the Austrian DPA ruled that the calculation of the credit score was to be considered profiling. It ruled that therefore the agency was obliged to provide information on the logic behind calculating the credit score pursuant to Article 15(1)(h) GDPR.	4 August 2021	Link to report by noyb (English)

Development	Summary	Date	Links
	Only the computer code supporting the calculation was protected as a trade secret. It is expected that the credit agency will appeal against this decision. Therefore, the decision is not yet binding.		
Austrian DPA issues fine of EUR 9.5 million for violating right of access	According to news reports, the Austrian DPA has issued a fine of EUR 9.5 million against a postal services organisation for unlawfully refusing to respond to DSARs that were sent via email. The DPA considers this a violation of data subjects' right of access under Article 15 GDPR. The postal services organisation has announced it will appeal against this decision. Therefore, the decision is not yet binding.	29 September 2021	Link to news report (German)



China

Contributors

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

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

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

Development	Summary	Date	Links
Measures for cybersecurity reviews (Revision draft for comments) 《网络安全审查办法（修订草案征求意见稿）》	On 10 July 2021, the Cyberspace Administration of China ("**CAC**") published a revised draft of the Measures for Cybersecurity Reviews ("**Revision Draft Measures**") for public comment. Set out below are the key differences of the Revision Draft Measures compared to the previous draft. – The Revision Draft Measures extend the possible subjects of cybersecurity review to include data processors whose processing activity affects or may affect national security, in addition to critical information infrastructure operators procuring network product or service (collectively "operators") from the previous draft. – The Revision Draft Measures confer significance on cybersecurity reviews during listing. Operators in possession of personal information of more than 1 million users must apply for a security review if they wish to list outside the country. Accordingly, the China Securities Regulatory Commission was also recently added to the list of regulatory authorities tasked with jointly coordinating cybersecurity review related matters. – During a cybersecurity review, which focuses on evaluating potential national security risk, a multitude of factors would be taken into account. Examples of new additions include:	10 July 2021	Measures for cybersecurity reviews (revision draft for comments)

Development	Summary	Date	Links
	the risk that crucial or large amounts of personal information may be influenced, controlled or maliciously manipulated by foreign government after overseas listing, or the risk of it being stolen, leaked, damaged, illegally used or transmitted overseas. – Regarding procedural matters, the Revision Draft Measures extend the special review period from 45 working days (as in the previous draft) to 3 months, subject to extension if further complications arise.		
Administrative provisions on security vulnerabilities in network products 《网络产品安全漏洞管理规定》	On 12 July 2021, the Ministry of Industry and Information Technology ("**MIIT**"), the CAC and the Ministry of Public Security jointly published a circular on the issuance of the Administrative Provisions on Security Vulnerabilities in Network Products ("**Administrative Provisions**"). The Administrative Provisions apply to three main types of entities, namely: network products (including hardware and software) providers; network operators; and individuals or organisations engaging in the detection, collection and publication of security vulnerabilities. The Administrative Provisions impose the following general and specific obligations on these entities: General obligations: – All three classes of entities are required to maintain a channel for receiving reports of security vulnerability in their network products and shall preserve such information for no less than six months. Specific obligations of network products providers: – They are required to take steps to ensure a timely repair and reasonable publication of any security vulnerabilities and provide users with proper guidance and support in taking precautionary measures. The Administrative Provisions highlight proper evaluation, informing, reporting and vulnerability fixing obligations.	1 September 2021	Administrative provisions on security vulnerabilities in network products

Development	Summary	Date	Links
	Specific obligations of individuals or organisations engaging in the detection, collection and publication of security vulnerabilities: – When publishing information on any detected security vulnerability via network platform, media, conference etc. they shall abide by the principles of necessity, honesty, impartiality and furthering cybersecurity risk prevention. The Administrative Provisions lay out eight specific requirements, for instance, "white hats" are not allowed to make an early release of the security vulnerability before a fix is devised; prohibition against intentionally exaggerating the risk or exploiting information for malicious purposes; and seeking State approval prior to publication during a major event etc. – As for liabilities, the Administrative Provisions make reference to the PRC Cybersecurity Law. Network products providers in violation shall face a fine of up to RMB 500,000 whereas responsible individuals could face up to RMB 100,000. For network operators that fail to act to repair or prevent security vulnerabilities they may face a fine of up to RMB 100,000 with responsible individuals facing up to RMB 50,000.		
Provisions of the Supreme People's Court on Several Issues concerning the application of law in the trial of civil cases involving the processing of Personal Information using facial recognition technology《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》	On 27 July 2021, the Supreme People's Court published the provisions of the Supreme People's Court on several issues concerning the application of law in the trial of civil cases involving the processing of Personal Information using facial recognition technology ("**Interpretation**"), imposing stricter data protection requirements. The Interpretation highlights a range of scenarios of processing facial information which could constitute an infringement of personal rights. These include: – utilising facial recognition technology to verify, identify or analyse faces in public areas (eg hotel, shopping mall, bank, airport etc.) in violation of laws or regulations; – failing to disclose or specify the rules, purpose, manner or scope of such processing;	1 August 2021	Provisions of the Supreme People's Court on Several Issues concerning the application of law in the trial of civil cases involving the processing of Personal Information using facial recognition technology

Development	Summary	Date	Links
	– failing to obtain the requisite consent of data subjects or their guardian; – processing facial information contrary to the agreed purpose, manner or scope; – omitting to take measures in safeguarding information security resulting in leak, interference or loss of information; – providing information to other parties in violation of any law, regulation or agreement; – processing facial information in a manner that would violate public order or ethics, and – processing facial information in a manner that would violate legality, legitimacy or necessity. More specifically, the Interpretation goes further to exclude certain circumstances where even consent would not constitute a valid defence. These are: – providers mandating consent as a pre-requisite to providing products or services, but where processing of facial information is not necessary; – bundled consent alongside other authorisations; and – consent obtained through force or disguise. Standard contracts requiring an individual to grant unlimited, irrevocable and freely transferrable consent to process facial information may also be invalid. Liabilities for non-compliance vary. An aggrieved data subject may claim for monetary remedies (including reasonable expenses and attorney's fees), request the processer deletes the relevant facial information and seek injunctive relief.		
Regulations on the security protection of critical information infrastructure **《关键信息基础设施安全保护条例》**	On 30 July 2021, the State Council published the Regulations on the Security Protection of Critical Information Infrastructure (**"Regulations"**). Scope of Critical Information Infrastructure ("**CII**"):	1 September 2021	Regulations on the security protection of critical information infrastructure

Development	Summary	Date	Links
	Generally, CII is contemplated to be key network facilities and information systems in certain industries (eg public telecommunications and information services, public services, finance etc) that in the event of any destruction, loss of function or data leakage, may seriously endanger national security. Identification of CII: Relevant security protection departments are empowered to formulate rules for identification of CII taking into account the following factors: – degree of importance to the core operations of the industry/area; – potential degree of damage following a destruction, loss of function or data leakage; and – corresponding impacts on other industries and areas. Key obligations of CII operators: CII operators are bound by a series of obligations under the Regulations, which includes: putting in place a sound cybersecurity protection system and accountability system; establishing a dedicated security management body; and conducting at least one network security test and risk assessment annually, and rectifying and reporting accordingly. Liabilities for non-compliance: Both CII operators and their responsible persons may face repercussions for non-compliance. CII operators may be subject to a correction order, warning, monetary fine and confiscation of the illegal income. Individuals responsible for such non-compliance may also have a fine or detention imposed on them and/or be prohibited from future employment in core positions related to cybersecurity administration and network operations, as well as various other criminal liabilities under applicable laws.		
Provisions on vehicle data security management (for trial	On 16 August 2021, the CAC, National Development and Reform Commission, MIIT, Ministry of Public Security and Ministry of Transport jointly released the Several Provisions on Vehicle Data Security Management (for Trial Implementation) ("**Provisions**").	1 October 2021	Several provisions on vehicle data security management (for trial implementation)

Development	Summary	Date	Links
implementation) **《汽车数据安全管理若干规定（试行）》**	We summarise below the updates to the Provisions compared to their previous drafts. Scope of application and definitions: The Provisions include an explanation of their scope of application with more refined definitions that are also more in line with the relevant laws. These include: – replacing "operators" with "vehicle data processors". The term, alongside examples provided in the Provisions (including automobile manufacturers and repair and maintenance providers), covers almost all operators in the whole chain of the automobile industry; – notably, aligning its definitions for personal information and sensitive personal information with the Personal Data Protection Law ("**PDPL**"), with tweaks made to pertain to vehicles; and – amending the scope of important data, including: adding the requirement of "reflecting performance of the economy" before classifying any data on traffic volume and logistics as important data, and excluding "surveying information with a higher level of precision than maps published by the State" from the scope which was initially written under the draft. Principles of Processing of Personal Data: Following the five principles as introduced in our previous update, the Provisions made slight adjustments as follows: – providing flexibility to the default non-collection of data by removing the previous limitation on frequency of consent under the draft; – expanding the principle of anonymisation to include all aspects related to the processing of vehicle data (and not merely to before providing information to outside the vehicles); and – deleting the minimum retention period principle. Requirements for Processing Personal Information:		

Development	Summary	Date	Links
	The Provisions made slight updates to the content of the notice to be given to the data subject and require consent when processing personal information. Similarly, updates were made to the requirements for processing sensitive personal information. In particular, the Provisions provide for an exception to consent. This exception can only be invoked when there is a need to ensure driving safety and if it pertains to collection of data from individuals outside the vehicle. Data Localisation: Last but not least, the Provisions have removed the previous restrictions on requiring operators to take steps to ensure data security and prevent the loss of data in the event that scientific and commercial ventures acquire and utilise personal information and important data stored within PRC. The idea behing this is to better facilitate reasonable commercial development and usage of vehicle data.		
Personal Data Protection Law of the PRC **《中华人民共和国个人信息保护法》**	On 20 August 2021, the Standing Committee of the National People's Congress of China published the PDPL. We summarise below the key updates to the finalised legislation compared to the second draft. Legal basis for processing personal data: The PDPL now has a total of seven legal bases for data processing. Compared to the second draft, the only substantial update is to the contractual necessity ground, which would also extend to human resources management under a legally established policy or legally concluded collective contract. Separate consent: The PDPL has consistently throughout its previous two drafts and in the final version introduced the requirement of separate consent. Most notably, processors would need to obtain separate consent from a minor's guardian when processing personal information of a minor below the age of 14, as such information is now recognised to be sensitive personal information. Cross-border data transfer:	1 November 2021	Personal Data Protection Law of the PRC

Development	Summary	Date	Links
	The PDPL would allow the transfer of information outside the PRC if any international treaty or agreement concluded or acceded to by the PRC so provides or requires. Personal information processors are required to go the extra mile by ensuring that the processing activities of the foreign recipients confer a comparable standard of protection as to the PDPL. When responding to requests from overseas judicial or law enforcement agencies, the competent authorities of the PRC shall handle such requests in accordance with the relevant laws or international treaties or agreements, and in compliance with the principles of equality and reciprocity. Protection of data subjects: The PDPL confers specific protection under certain scenarios, these include: – Rights of deceased persons: The final PDPL drastically changes the concept of data protection rights initially introduced in the second draft. After implementation, a close relative may, for their own lawful and legitimate interests, access, copy, amend or delete such information, unless the deceased has specified otherwise before death; – Automated decisions: Automated decisions shall not subject individuals to unreasonable differential treatment, including price and conditions; – Transfer of data: Individuals have the right to request their personal information be transferred to a processor designated by them, provided that the processor meets the conditions of CAC; – Legal entitlements: A data subject may file a claim in a people's court against a personal information processor refusing to respond to requests exercised pursuant to his/her rights. Personal information protection mechanisms: The final PDPL imposes a wider range of information protection mechanisms on personal information processors. For example, the notification obligation would be triggered not only after the actual occurrence of an incident, but also when it is likely to		

Development	Summary	Date	Links
	occur. Further, tampering, in addition to leakage or loss, would also be considered an incident triggering notification. In case of personal information leakage, falsification or loss, the notice to be issued by the processor would be extended to also include the types and causes of such incident, its possible harm, and remedial measures taken for mitigation.		
Administrative provisions on algorithm recommendation of the Internet Information Services (draft for comments) **《互联网信息服务算法推荐管理规定（征求意见稿）》**	On 27 August 2021, the CAC published the Administrative Provisions on Algorithm Recommendation of Internet Information Services (Draft for Comments) ("**Draft Provisions**") for public comment. The Draft Provisions apply to and govern the use of algorithmic recommendation technology in providing internet information services within the PRC. Such use is defined as providing information content to users through generation and synthesis, personalised pushing, sequence selection, search filtering, and adjusting decision-making. The Draft Provisions stress the principle of mainstream values, and contributions for a better and more positive algorithm mechanisms landscape. Service providers are bound by a set of general obligations, including: – implementing entity responsibility for algorithm security, establishing competent management systems, allocating professional support and publishing algorithm recommendation guiding rules; – periodically reviewing algorithm mechanisms and refraining from setting up models that would cause addictions or go against public customs; – strengthening the management of information content, preventing dissemination of illegal content, and retaining and reporting relevant records; – strengthening the management of user modelling and labels and fending off unlawful, negative or discriminatory labels – enhancing the ecological management of recommendation pages; and – optimising strategies and transparency.	1 November 2021	Administrative Provisions on the algorithm recommendation of the Internet Information Services (draft for comments)

Development	Summary	Date	Links
	On a more specific set of "dos" and "do nots" – first, the Draft Provisions prohibit the use of algorithms for unfair competition. Service providers are not allowed to give a false impression of web traffic (eg by creating fake accounts) and manipulating search results (eg blocking information and making excessive recommendations). Furthermore, the Draft Provisions offer special protection to certain groups, namely: – consumers from being subject to unreasonable treatment differentiation in transaction price and other conditions; – minors are shielded from information detrimental to their physical and psychological health and are further exposed to beneficial and healthy information; and – employees subject to work scheduling shall enjoy better order allocation, payments and work times. Penalties for non-compliance vary according to the specific provision violated. Possible penalties would include warnings, criticisms circulation, order correction, suspension of information updates, fines, revoking filings, public security administrative sanctions and criminal responsibility in accordance with applicable PRC laws.		
Administrative measures for record-filing of the platforms for collection of security vulnerabilities in network products (draft for comments) **《网络产品安全漏洞收集平台备案管理办法（征求意见稿）》**	On 13 September 2021, the MIIT published the Administrative Measures for Record-filing of the Platforms for Collection of Security Vulnerabilities in Network Products (Draft for Comments) ("**Draft Measures**") for public consultation. Platforms for collection of security vulnerabilities in network products refer to platforms by organisations or individuals established to collect security vulnerability information in respect of network products other than their own. The Draft Measures expressly exclude from its scope platforms that are only used for repairing security vulnerabilities of their own network, network products and systems. The Draft Measures require individuals or organisations seeking to establish a platform for collection of security vulnerabilities to file certain specified information with the MIIT prior to its actual operations. Platforms that are already in operation shall file	13 September 2021	Administrative measures for record-filing of the platforms for collection of security vulnerabilities in network products (draft for comments)

Development	Summary	Date	Links
	accordingly within ten working days of the effective date of the Measures. The Draft Measures also set out the procedures following verification of information by the MIIT, and procedures to be adopted by the relevant platform in the event of any change to the filed information or termination of business.		
Information security technology – Identification guide of important data (draft for comments) **《信息安全技术** **重要数据识别指南（征求意见稿）》**	On 23 September 2021, a draft recommended national standard, "Information Security Technology – Identification Guide of Important Data (Draft for Comments) (信息安全技术重要数据识别指南(征求意见稿))" ("**IGID**") was released. However, it is only an interim work product and does not reflect the authority's final opinion. The final version of the IGID may still be adjusted subject to further announcements by the CAC of the relevant rules. The IGID has listed 8 general characteristics for important data, which relate to the following areas: – economic operation; – human and health; – natural resource and environment; – science and technology; – security protection; – application service; – political activities; – others. The IGID further recommends that: (i) the relevant local or industrial authorities shall, based on the above general characteristics, formulate their own rules to identify the specific category and more detailed characteristics of its important data; (ii) all organisations may then identify their important data based on the detailed rules as mentioned in (i) and formulate an important data directory; and (iii) all organizations shall then report the identification result of their important data to the relevant local or industrial authorities.	23 September 2021	This IGID has only been released by some private sources and no official link is available at this stage.

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
Code of conduct: CNIL grants first approval to a monitoring body	On 17 June 2021, the CNIL delivered its first approval to a monitoring body tasked with ensuring the proper application of the first CNIL-approved code of conduct, which was developed by Cloud Infrastructure Service Providers Europe ("**CISPE**") and is dedicated to cloud infrastructure service providers ("**IaaS**"). The approval triggers the effective date of the CISPE code of conduct. The approval granted by the CNIL will remain in force for 5 years. However, in the event that the requirements relating to the approval are no longer complied with, the approval may be revoked. The CNIL is examining other applications by organisations wishing to become monitoring bodies for that code of conduct. Codes of conduct allow professionals in a given sector to demonstrate their compliance with the GDPR by justifying the good practices they have put in place. Adherence to a code is voluntary, but implies correct application of control measures by third party organisations. To implement this these organisations	CNIL's statement (in French): 23 September 2021 CNIL's deliberation (in French): 17 June 2021	CNIL's statement (French) CNIL's deliberation (French)

Development	Summary	Date	Links
	must be approved by the competent control authority on the basis of the CNIL's guidelines.		
Administrative fine of EUR 1,750,000 for insufficient information to individuals and excessive data retention	On 20 July 2021, the CNIL sanctioned a French company specializing in the management of complementary pensions for private sector employees and assurance. Inspections carried out by the CNIL in 2019 showed that the company stored clients' personal data for an excessive period of time, and failed to properly inform data subjects of privacy related information when the company carried out telephone solicitation campaigns. The CNIL first found that the company failed to comply with the obligation not to retain personal data for longer than necessary under Article 5.1 (e) GDPR, as it kept the data of clients longer than the maximum period allowed by French law and the data of prospective clients for more than three years. In addition, the CNIL found that the privacy notice information provided to individuals contacted by phone by the company's subcontractors was insufficient (Articles 13 and 14 GDPR). In particular, phone calls could be recorded without the individual being informed of the recording or of the right to object to such recording. The amount of the fine was EUR 1,750,000, which was assessed taking into account the size and financial situation of the company in order to impose a dissuasive and proportionate fine.	CNIL's statement (in French): 23 September 2021 CNIL's deliberation (in French): 20 July 2021	CNIL's statement (French) CNIL's deliberation (French)
Administrative fine of EUR 400,000 for failure to inform political figures, journalists and activists of data collected for lobbying purposes	In July 2021, the CNIL issued an administrative fine of EUR 400,000 against a leading company specializing in the field of plant biotechnology. In May 2019, the press revealed that the company held personal data of more than 200 politicians, journalists, environmental activists, scientists etc. involved in a debate about the renewal of approval granted by the European Commission for the use of glyphosate (a herbicide) in Europe. The CNIL then received complaints from seven concerned individuals who claimed that they had not been informed of that practice.	CNIL's statement (in French): 23 September 2021 CNIL's deliberation (in French): 26 July 2021	CNIL's statement (French) CNIL's deliberation (French)

Development	Summary	Date	Links
	Inspections carried out by the CNIL showed that the data had been compiled on behalf of the company by several lobbying organisations. The data included the individuals' organisation, job title, professional address, professional landline number, mobile phone number, email address and, in some cases, Twitter account. In addition, each individual was given a score ranging from 1 to 5 to assess their influence, credibility and support to the company on various subjects such as pesticides or genetically modified organisms. While the CNIL pointed out that the collection of such data for lobbying purposes was not, in itself, unlawful, it considered that the company breached the GDPR because it both failed to inform the concerned data subjects in accordance with Article 14 GDPR so that they could exercise their right of opposition and because it did not enter into an agreement with the lobbying organisations as mandated by Article 28 GDPR. Interestingly, the CNIL considered that informing the data subjects would not require disproportionate effort, as the data included the contact details of all the data subjects. It further recalled that information is an essential right as it communicates details relating to the exercise of other rights (access, opposition, deletion etc.) to which data subjects are entitled.		
Fine of EUR 50,000 for placing cookies on website users' devices without their prior consent	In July 2021, the CNIL imposed a fine of EUR 50,000 on a company publishing a French news website for automatically placing advertising cookies on the devices of the website's users without obtaining their prior consent. The CNIL carried out inspections in 2020 and 2021 on the company's website, and found that, when users visited the website, third-party cookies were installed by partners of the company on their devices before they provided consent, but also when they refused to accept cookies. The CNIL outlined that the publishing company was responsible for ensuring that its partners comply with the rules applicable to cookies, and should have made its best efforts to ensure that they did not place advertising cookies on the website users' devices before the users had accepted these cookies. According to the CNIL, the fact that the advertising cookies were placed on	CNIL's statement (in French): 23 September 2021 CNIL's deliberation (in French): 27 July 2021	CNIL's statement (French) CNIL's deliberation (French)

Development	Summary	Date	Links
	the users' devices by third parties could not exempt the website publisher from liability, since it was controlling the website and servers. The CNIL also considered that the tools implemented by the publishing company, such as a cookie management platform, were not sufficient since cookies which required consent were still installed before any consent was obtained or despite the refusal of the website's users. Therefore, the CNIL ruled that the publishing company infringed the provisions of the French Data Protection Act that implements into French law the provisions of the e-Privacy Directive relating to cookies. It underlined that this decision is part of its overall strategy on cookies, initiated in 2019 and aimed at ensuring that both French and foreign companies with websites directed towards French users comply with the requirement to lawfully obtain prior consent for cookies.		
CNIL's model for data protection maturity self-assessment	The CNIL released a data protection management maturity self-assessment model. The draft model transposes the maturity levels for information technology defined in international standards to data protection management. It aims to illustrate, for typical data protection actions implemented by organisations, each maturity level with examples of practices and processes. The model first sets out five levels of maturity to assess how well data protection actions are managed, ranging from (0) not performed, (1) performed informally, (2) planned and tracked, (3) well defined, (4) qualitatively controlled, and (5) continuously improving. It then describes eight typical data protection actions that may be put in place by organisations such as defining and implementing data protection practices, mapping and maintaining an accurate record of data protection activities, and responding to subject access requests. Most importantly, the model applies the levels of maturity to the typical data protection actions: a table illustrates, for all eight data protection actions, each maturity level with examples of practices and processes. Thus, it displays different degrees of robustness and sophistication for how actions related to data protection may be managed.	9 September 2021	CNIL's statement (French) CNIL's model (French)

Development	Summary	Date	Links
	The CNIL highlights that the model allows organisations to assess their own level of maturity and determine how to improve their management of data protection to reach a targeted adequate level. The model is, however, not intended to provide a guarantee of de facto compliance.		
New verifications of the CNIL relating to compliance with cookie regulations	In July 2021, the CNIL sent formal notices to approximately forty publishers of high-traffic websites whose practices on cookies was found to be contrary to the CNIL's new guidelines (published on 1 October 2020 with a 1 April 2021 effective date). One of the main tenets of these guidelines requires website publishers to ensure that their users can refuse cookies as easily as they can accept them. The companies that received formal notices were required to put their websites in compliance with the CNIL's guidelines before 6 September 2021. In September 2021, the CNIL indicated that thirty of these companies modified their practices to comply with its requirements, but that four failed to reply to the formal notices and were liable for potential administrative fines amounting to up to 2% of their global annual turnover. The CNIL indicated that it will continue to carry out verifications on the use of cookies by French and international entities operating in various sectors (the formal notices sent in July 2021 were directed to companies publishing retail websites, online travel agencies, car rental companies and companies operating in the banking and energy sectors).	14 September 2021	CNIL's statement (French)
Right to rectification and erasure enforced by the CNIL	Despite its small size, a French company was issued a EUR 3,000 fine by the CNIL because it was found to have breached several basic obligations under the GDPR, including the obligation to properly inform individuals (Articles 13 and 14 GDPR), compliance with the right to rectification and erasure (Articles 16 and 17 GDPR), maintaining a record of processing activities (Article 30 GDPR) and cooperating with the supervisory authority (Article 31 GDPR).	CNIL's statement (in French): 14 September 2021 CNIL's deliberation (in French): 15 September 2021	CNIL's statement (French) CNIL's deliberation (French)

Development	Summary	Date	Links
	This sanction and the fact that it was made public by the CNIL signals its intent to send a message that no company is too small to comply with the GDPR.		
CNIL launches a public consultation on a draft guide on recruitment	The CNIL recently published a consultation on a draft guide to help recruitment professionals comply with data protection obligations. In 2002, the CNIL published a first recommendation "relating to the collection and processing of personal information during recruitment operations" (deliberation n° 02-017 of 21 March 2002). However, the evolution of the legal framework, practices and technologies required an update of this position as well as clarification of new topics. This new guide is divided into 19 factsheets aimed at reviewing the basic and core topics of the regulation on data protection in the recruitment sector as well as providing answers to questions resulting from the use of new technologies by recruiters and certain other specific questions. Among those are "Can a recruiter use personality assessment tools or data available on social networks?"; "Under what conditions can video interviews be conducted?"; and "What rules apply to the collection of criminal records, mandatory checks or the collection of sensitive data such as health, religion or sexuality?" The consultation is open until 19 November 2021 to all recruitment stakeholders, both public and private (direct employers, recruitment firms, temporary work companies, platforms, etc.). The publication of a final guide is scheduled for February 2022.	20 September 2021	CNIL's statement (French) CNIL's draft guide (French)

Germany

Contributors

Alexander Niethammer
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

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

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

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

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

Isabella Norbu
Associate
T: +49 89 54565 191
isabellanorbu@
eversheds-sutherland.com

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

Development	Summary	Date	Links
GDPR damages only upon proof of specific damage by data subject	In accordance with the rulings of numerous other German courts, the Brandenburg Higher Regional Court has now also decided that a specific damage must be sustained in order to assert a claim for damages under the GDPR. For example, it is not sufficient if a photo and the name of the data subject are used on a website without permission. Rather, the data subject must prove which specific disadvantages he or she has suffered as a result.	11 August 2021	Judgment (German only)

Development	Summary	Date	Links
Improper use of a GDPR right to information	Requests for information from data subjects that are improper and serve solely to tie up the company's capacities are a problem of practical relevance for companies. The Wuppertal Regional Court has now defined when a right to information under Art. 15 GDPR is improper. Since the right to information is intended to enable the data subject to be aware of the processing of his or her personal data and to be able to check its lawfulness, requests for information that pursue a purpose other than data protection are inadmissible.	29 July 2021	Judgment (German only)
Mandatory consent to advertising in online lotteries is permissible	The Data Protection Commissioner of North Rhine-Westphalia states in her activity report that online lotteries, where the data subject has to give mandatory consent to advertising, are legally valid. Although there is no valid consent because the consent is not freely given, a contract between the data subject an the controller can be referred to as the legal basis.	1 July 2021	Activity report (p. 40)
Compensation for damages in the event of insufficient GDPR information	An employer requested her employer to grant her information pursuant to Art. 15 GDPR. However, the employer did not sufficiently comply with this request. For this reason, the Regional Labour Court of Hamm awarded the woman damages in the amount of EUR 1,000. According to the court, there was no exception for minor cases.	11 May 2021	Judgment (German only)
Requirements on effective consent to telephone advertising	In its ruling, the Bonn District Court defined the requirements for effective consent to telephone advertising. The controller collected the opt-in in the context of an online sweepstake. Considering this, it must first be possible for the data subject to determine to whom exactly the consent to advertising is to apply. Consumers have a legitimate interest in receiving sufficiently detailed information about the type of services or products and the companies from which they will receive advertising in a specific case.	22 September 2020	Judgment (German only)
Proceedings of the Berlin data protection authority against unlawful tracking	The Berlin Commissioner for Data Protection and Freedom of Information announced in a press release that approximately 50 Berlin companies have been warned for using unlawful tracking technologies. Unless the companies concerned review their websites and bring the tracking in line with current data	9 August 2021	Press statement (German only)

Development	Summary	Date	Links
	protection regulations, a formal investigation will take place and fines may be imposed.		
Fine due to insufficient technical-organisational measures	The Data Protection Commissioner of Lower Saxony announced in her most recent activity report that she had imposed a fine of EUR 65,500 on an online shop due to its insufficient technical and organisational measures. The shop used a web shop application that had been outdated for many years and had significant security failings.	1 August 2021	Activity report (German only)
Right of the controller to refuse information in the event of requests for information from data protection authorities	The Higher Administrative Court of Schleswig-Holstein ruled that a company does not have to incriminate itself if a data protection authority requests information. Rather, it can refuse to provide the information. However, this only applies to questions where there is a risk of criminal proceedings or an administrative offence. Failure to respond to the request for information, however, entails the risk of an extensive on-site data protection audit by the authority.	28 May 2021	Judgment (German only)
Sending faxes is an insecure means of communication	In a statement, the Hessian data protection commissioner has spoken out against the transmission of personal data by fax, as there are now many more secure methods of exchanging messages, such as encrypted e-mail. A particular problem is that by entering a wrong fax number, personal data can be disclosed to third parties without authorisation. This results in risks to the rights and freedoms of data subjects that are not in line with the GDPR. Accordingly, the Hessian Data Protection Commissioner recommends, as a matter of principle, not to transfer personal data by fax and to switch to digital solutions. Only in exceptional cases, e.g. due to a particular urgency and if additional protective measures have been taken at the senders' and recipients' premises, should fax be used.	14 September 2021	Statement (German only)
Warning against the use of Zoom in the on-demand variant	The Hamburg Commissioner for Data Protection and Freedom of Information has officially warned the Senate Chancellery of the Free and Hanseatic City of Hamburg about the use of the video conferencing solution of Zoom Inc. in its on-demand variant. This violates the GDPR, as such use involves the transfer of personal data to the US. There is no sufficient protection for such data in this third country. In this way, the data of call participants are	16 August 2021	Press statement (German only)

Development	Summary	Date	Links
	exposed to the risk of mass surveillance in the US, against which there are no sufficient legal protection options. The European Data Protection Board has produced recommendations on the transfer of personal data to third countries such as the US in accordance with the GDPR.		

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

Clive Lam
Trainee Solicitor
T: +852 2186 3283
clivelam@
eversheds-sutherland.com

Catherine Wang
Trainee Solicitor
T: +852 2186 4939
catherinewang@
eversheds-sutherland.com

Development	Summary	Date	Links
PCPD issues guidance on Ethical Development and Use of Artificial Intelligence	On 18 August 2021, the Privacy Commissioner for Personal Data ("**PCPD**") published its "Guidance on the Ethical Development and Use of Artificial Intelligence" to facilitate the development and use of Artificial Intelligence ("**AI**") in Hong Kong and to assist organisations in complying with the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") in their development and use of AI. The guidance is structured in three main parts: (i) data stewardship values; (ii) ethical principles for AI; and (iii) recommended practices for organisations.	18 August 2021	Guidance on the Ethical Development and Use of Artificial Intelligence PCPD's media statement

Development	Summary	Date	Links
	Data stewardship values refers to being: (i) respectful; (ii) beneficial; and (iii) fair, and should represent the starting point for formulating ethical principles and practices for the development and use of AI. By reference to the above and their own corporate values, organisations shall then adopt appropriate ethical principles for AI. The ethical principles the PCPD encourages organisations to adopt are: – accountability; – human oversight; – transparency and interpretability; – data privacy; – fairness; – beneficial AI; and – reliability, robustness and security. The guidance also recommends practices for organisations to adopt in relation to the use and development of AI throughout the life cycle of their business processes, namely: – establishing AI Strategy and Governance; – conducting risk assessment and determining the level of human oversight; – developing AI models and management of AI systems; and – communicating and engaging with stakeholders. Aside from the above, the guidance also sets out a self-assessment checklist to assist organisations in determining whether the practices recommended in the guidance have been adopted in their development and use of AI.		
Gazettal of Personal Data (Privacy) (Amendment) Bill 2021	On 16 July 2021, the Hong Kong government gazetted the Personal Data (Privacy) (Amendment) Bill 2021 (the "**Bill**"). The Bill was introduced into the Legislative Council for the first and second reading on 21 July 2021.	16 July 2021	Personal Data (Privacy) (Amendment) Bill 2021 Government's press release

Development	Summary	Date	Links
	The Bill aims to combat acts of doxxing by criminalizing such acts. Under the Bill, anyone who discloses an individual's personal data without the consent of the data subject with an intent to cause specified harm, or who is reckless about the harm caused, will violate the provisions of the Bill. "Specified harm" refers to: (i) harassment, molestation, pestering, threat or intimidation to the person; (ii) bodily harm or psychological harm to the person; (iii) harm causing the person reasonably to be concerned for the person's safety or well-being; or (iv) damage to the property of the person. Other key matters set out in the Bill include the following: – the Bill grants the PCPD statutory powers to issue cessation notices demanding to cease or restrict the disclosure of doxxing content, conduct criminal investigations and institute prosecution with regards to doxxing cases and to require the delivery of materials and provision of assistance for doxxing cases; – the Bill mandates electronic platforms to comply with cessation notices issued by the PCPD to ensure prompt removal of doxxing content. The HK government has provided that the Bill is not intended to target service providers; and – the Bill also provides for ancillary offences such as non-compliance with a cessation notice, secrecy obligations or obstruction, hindrance or resistance to investigations. In a media statement issued by the government, it stated that in drafting the Bill, the government also made reference to the relevant laws of other jurisdictions such as Singapore, Australia and New Zealand. The current Bill does not address other proposed amendments previously discussed such as mandatory data breach notifications and data retention requirements. It remains to be seen if such proposed amendments would be introduced at a later stage.		

Hungary

Contributors

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

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

Kinga Mekler
Senior Associate
T: +36 13 94 31 21
mekler@
eversheds-sutherland.hu

Development	Summary	Date	Links
Data protection authority's statement on the lawfulness of asking for proof of vaccination against coronovirus in order to attend a theatre performance	On 13 September 2021, the Hungarian Data Protection Authority ("**DPA**") published a statement on the lawfulness of asking for proof of vaccination against coronovirus in order to attend a theatre performance, under the GDPR. The processing of health data is prohibited under the GDPR. Data relating to an individual's vaccination againt coronavirus is considered health data, therefore its processing is generally prohibited. According to the Section 2/A. § of the Government Decree No. 484/2020 (XI. 10.) during the second phase of protection measures applied during the state of emergency: "If a right under this Decree may be exercised in the event of protection against coronavirus the person intending to exercise that right may be required to present the certificate of immunity in such a way as to prove that he is entitled to exercise that right." The Government Decree defines such obligations in connection with attending events. For the purposes of this Decree, a cultural event shall not be considered an event if, for the purpose of performing art: – it is held in a place reserved for that art;	13 September 2021	DPA Statement

Development	Summary	Date	Links
	– it is open to the public against payment of a pre-booked seat ticket; and – the spectator must remain in his or her pre-booked seat for the duration of the performance. This defines theatre performances as: "performances held for the purpose of performing art". As theatre performances do not fall within the definition of "event" under Government Decree No. 484/2020 (XI.10.), there is currently no legal requirement for theatres to obtain proof of vaccination, so they cannot lawfully invite data subjects to do this.		
Data protection authority's statement regarding universities requesting vaccination certificates from students, as a condition for residence in dormitories and attending events	On 30 July 2021 the DPA published a resolution on the request by unviersities for vaccination certificates for coronavirus from students, in connection with dormintory accomodation and university events. The DPA notes that the legislation in force at the time of the adoption of the statement does not impose any obligation on higher education institutions to know or verify vaccination status. In the DPA's view, vaccination status, or lack thereof, constitutes health data. In the absence of specifically defined conditions and consequences, higher education institutions cannot lawfully require proof of protection against the coronavirus as a condition for residence in a dormitory In the DPA's view – on the basis of the legislation in force – it is not sufficient for the university to merely be interested in knowing this information and record whether students and staff have received a vaccination.	30 July 2021	DPA Statement

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
Commencement of certain provisions of the Data Sharing and Governance Act 2019	Many of the compliance requirements set out in the Data Sharing and Governance Act 2019 ("**DSG Act**") were not implemented when the DSG Act was originally enacted in 2019. On 7 July 2021, a number of key compliance provisions contained in the DSG Act were commenced. The key areas commenced include part 4 of the DSG Act which sets out specific requirements which must be included in a data sharing agreement and part 9 of the DSG Act on data governance, which has the effect of establishing the Data Governance Board. Please see our article "Data Sharing between public bodies: Five key updates" at the link provided for more information.	7 July 2021	DSG Act Data Sharing between public bodies: Five key updates
The Joint Committee on Justice ("Committee") publishes a report on the DPC	The Committee published a report on the GDPR which includes recommendations on the work of the Irish Data Protection Commission ("**DPC**"). These recommendations come on foot of the Committee's finding that several elements of the DPC's procedures require "attention and reform". The recommendations include advising the DPC to urgently move from emphasising guidance to emphasising enforcement, and to increase the use of its sanctioning powers to ensure effective implementation of the GDPR. The full text of the report is available at the link provided	22 July 2021	Committee Report
The EDPB publishes a binding decision addressing the DPC's draft	In December 2018, the DPC commenced an inquiry to consider whether a messaging app had discharged its GDPR transparency	28 July 2021	EDPB Decision

Development	Summary	Date	Links
decision regarding messaging app and DPC announces final decision	obligations with regard to the provision of information, and the transparency of that information, to both users and non-users of the app's service. The EDPB published its decision on the Irish DPC's draft decision on the inquiry. The decision sought to address the dispute that arose when the Irish DPC requested feedback from other jurisdictions under Article 60 GDPR. The EDPB came to the conclusion that the DPC should amend its draft decision regarding infringements of transparency, the amount of the fine, and the period given to the app to comply with the order. The full decision is available at the link provided. The DPC imposed an administrative fine of EUR 225 million, and has ordered the app to bring its processing into compliance with the GDPR by taking a range of specified remedial actions. The full decision is available at the link provided.		DPC Decision
The DPC publishes guidance on redacting documents and records	The DPC has published guidance entitled "Redacting Documents and Records" where it sets out general principles for redacting, along with more specific advice with regards to applying redactions to paper documents and electronic documents. The DPC recommends that regardless of the document type the redaction should be done on a copy version of the document and records detailing a clear description of what was redacted along with why it was redacted should be retained. The full guidance is available at the link provided.	28 August 2021	DPC Guidance
The DPC launches two inquiries into social media company concerning compliance with GDPR requirements relating to the processing of children's personal data and transfers of data to China	Pursuant to section 110 of the Data Protection Act 2018, the DPC has launched two inquiries into a soci media platform's compliance with GDPR requirements. The first inquiry will focus on compliance with the data protection by design and default requirement under GDPR as they relate to platform settings for users under age 18 and age verifications for children under 14. The second inquiry will examine transfers of personal data to China by the platform and compliance with GDPR requirements for transfers of personal data to third countries.	14 September 2021	DPC Statement
The DPC announces new breach notification web-forms	Further to a review by the DPC of its breach notification forms available on its website, the DPC has announced that a revised web-form will be implemented. The revised breach web-form seeks to improve the ease of use for data controllers and to	15 September 2021	DPC Statement

Development	Summary	Date	Links
	reduce common errors or misunderstandings when breach web-forms are submitted to the DPC.		

Italy

Contributors

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

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

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

Development	Summary	Date	Links
IDPA Annual Report for 2020	The Italian Data Protection Authority ("**IDPA**") released its Annual Report for 2020. In the report, the IDPA published the data and the statistics of its activities over the year, which was inevitably focused on the response to the COVID-19 pandemic. Among its various interventions and measures, the IDPA reported on those measures it had implemented to protect minors online, so as to guard them against revenge porn and cyber-bullying, for example. The IDPA additionally discussed the use of measures deployed in the health sector regarding the processing of relevant health data, the efforts made to regulate public entities and enforce their data protection obligations, as well as the action taken against unlawful telemarketing (which included the issuing of fines totalling several millions of Euros).	2 July 2021	IDPA's press release (in Italian) IDPA's Annual Report (executive summary also available in English, document in Italian)
IDPA's fines food delivery company for breaches of data protection and employment law	After a long and complex investigation, performed in cooperation with the Spanish Data Protection Authority, the IDPA found a food delivery company liable for several relevant data protection law infringements, including infringement of Italian employment law. The IDPA focused on the algorithms used to handle employees' data, the IDPA found that the company had failed to adequately inform its employees on the functioning of the algorithmic system and had not implemented suitable safeguards to ensure accuracy and fairness of the results that were used to rate riders'	Date of press release making available IDPA's measure: 2 July 2021 Date of IDPA's measure: 10 June 2021	IDPA's press release (with link to the English abstract of the measure) IDPA's measure n. 234 of 10 June 2021 (in Italian)

Development	Summary	Date	Links
	performance. The company also failed to provide adequate inform employees in respect that their geo-location data, work patterns and the orders assigned to them were being monitored. In addition, the IDPA found that the company had no procedures in place to enforce rights in relation to algorithmic decision-making (including the rights to obtain human intervention and to challenge the decisions) – which in some cases led to the exclusion of riders from work assignments. The IDPA found that there had been a number of other contraventions of the GDPR and the company had also failed to comply with its employment law obligations (including on monitoring of employees). The IDPA fined the company EUR 2.6 million and prescribed corrective measures.		
IDPA's new guidelines on cookies and other tracking devices	The IDPA has issued guidelines (or measure) on cookies and other tracking devices, based on the GDPR and Court of Justice of the European Union case law, as well as taking into account previous reports published and complaints received by the IDPA. The guidelines replace a previous measure from 2014. The IDPA remarks that before the acquisition of the user's consent, no cookie/other tracking device can be installed or used unless they are are strictly necessary to operate the website and to allow users to browse them. The IDPA has also provided clarification on how to inform data subjects about how their data is collected and on how to obtain their consent (generally prohibiting the use of cookie-walls or merely scrolling as a means to give consent and as a reiteration of requesting consent). The IDPA's measure was published in the Italian Official Journal on 9 July 2021 and controllers will have 6 months to comply with the IDPA's guidelines starting from that date.	Date of press release making available IDPA's guidelines: 2 July 2021 Date of measure providing IDPA's guidelines: 10 June 2021	IDPA's press release IDPA's guidelines on cookies and other tracking devices
IDPA measure on investigation initiatives for July-December 2021	The IDPA has published a new measure, providing a list of processing activities on which it will focus its investigations from July-December 2021 with the assistance of a specialist division of the Italian Tax Police. This list of activities includes, inter alia, processing activities concerning: – the processing of biometric data for facial recognition, including through CCTV systems;	22 July 2021	IDPA's measure n. 286 of 22 July 2021 (in Italian)

Development	Summary	Date	Links
	– the processing of personal data by "data brokers"; – the processing of personal data for marketing and profiling purposes; – the processing of personal data in respect of reputational databases; – the processing of personal data in the food delivery sector; – data breaches; and – controls on the requirements for the lawfulness of the processing, the conditions for consent and compliance with the obligation to provide information notices. This list above is without prejudice to any other investigation the IDPA may perform during the period, both ex officio and when following reports or complaints.		
IDPA's measure fining a food delivery company	IDPA issued a fine against a food delivery company in response to its unlawful processing of personal data of approximately 8000 delivery riders. IDPA found several infringements, including the lack of transparency of algorithms used to manage riders, to assign orders and to book working patterns. It emerged from the IDPA's assessments that the company monitored employees through geo-location tracking and stored a significant amount of data in breach of the Italian employment law requirements on employees' monitoring. IDPA made several enforcement orders to the company and issued a fine amounting to EUR 2.5 million.	2 August 2021	IDPA's newsletter making available the measure (in Italian) IDPA's measure n. 285 of 22 July 2021 (in Italian)

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
Royal Netherlands Marechaussee (Dutch military constabulary) may use ethnic profiling	In a case against the State regarding the use of ethnicity data in the Mobile Security Surveillance ("**MTV**") by the military constabulary, also known as the Royal Netherlands Marechaussee (**"Marechaussee"**), the court has ruled in favor of the Marechaussee on the issue of ethnic profiling. The proceedings against the State were initiated by multiple interest groups, including Amnesty International. These opposing parties argued that the Marechaussee, by carrying out these MTV checks, were carrying out unauthorised use of ethnicity data when conducting border controls, thus constituting discrimination. MTV is a form of immigration control at the internal borders of the European Union and the purpose of the system is to combat illegal residence in the Netherlands. MTV border control inspections often take place at airports, where there are flights coming in from EU Member States, and on roads and waterways at the borders with Germany and Belgium. The objective of the MTV is not to detect criminal offences, but rather to establish the identity, nationality and residence status of individuals. This is	22 September 2021	Court ruling (in Dutch)

Development	Summary	Date	Links
	permissible under Dutch law, even without having any basis for indications or suspicions of illegality. MTV's control actions are planned on the basis of general risk profiles, in which ethnicity does not play a role. On the basis of the risk profile, selection decisions are made during an action, whereby individuals are designated for a check. However, the Marechaussee does use ethnicity as a possible indicator when making such decisions. The court ruled that the manner in which this is done does not constitute discrimination. MTV checks are intended to determine the residence status of people, and therefore nationality can play an important role in determining the person's status, with ethnicity being a potentially objective indicator of an individual's supposed nationality. Ethnicity is not the only indicator used by the MTV and the selection decisions used have to be accounted for. Random checks or not checking and selecting at all do not offer a reasonable alternative for MTV control actions. Therefore, the court rejected the claim of a general prohibition on the use of ethnicity in MTV checks. The claimants have already announced that they will lodge an appeal against this ruling.		
DDPA's budget will not be increased in 2022	The Dutch Data Protection Authority ("**DDPA**") and the Dutch government have announced that the budget of the DDPA for 2022 will remain at EUR 25 million, the same as 2021's budget. The House of Representatives had adopted two motions in the past year to increase the budget of the DDPA and they had called upon the Dutch government to increase the budget of the DDPA. The House of Representatives argued that the current budget of EUR 25 million is insufficient to carry out all of the DDPA's tasks, and that the DDPA's budget must be increased to EUR 100 million, comparable to other Dutch supervisory authorities. However, the Dutch government has rejected the House of Representatives' proposal.	21 September 2021	DDPA statement (in Dutch)
Health insurance company changes its working method after DDPA investigation	A health insurance company is changing their working methods with respect to authorization requests following the outcome of an investgation in February 2020, whereby the DDPA ruled that the company's procedure for authorization requests was in violation of the GDPR. As background, through an application for authorization, the insurance holder can request the health	14 September 2021	DDPA statement (in Dutch)

Development	Summary	Date	Links
	insurer's prior approval for reimbursement of certain care. Such applications involve requests by insurance holders who need medical-specialist rehabilitation care. The DDPA ultimately found that the company was processing more health data than necessary to assess certain authorization requests that it had received. The insurance holder had to submit a range of personal details on the form, including information on their referral, indication, past treatments, the full treatment plan, the treatment objectives, the disciplines involved in the treatment and the treatments that needed to be declared. If the insurance holder did not provide the aforementioned information, the request would be refused and the company would not reimburse the costs. The DDPA imposed an order subject to a penalty for non-compliance with Article 5(1)(a), Article 6(1)(b) and Article 9(1) GDPR. The company has filed an appeal against the order. The company has also engaged in discussions with the DDPA about changing its standard operating procedure. Additional processing of health information may only be requested if the company has valid reasons to doubt the opinion of the attending rehabilitation medical-specialist. Health insurers like the company must substantiate this on a case-by-case basis, and only then can the health insurer request additional information from the insurance holder. The company is now following a new process, with new guidelines for the assessment of authorization requests for medical-specialist rehabilitation without admission.		
License granted to financial institutions by DDPA to share information on fraud	The DDPA has granted a license to more than 160 financial institutions – subject to strict conditions – to register and share details of fraudulent entities/individuals on an incident warning system. Fraudulent entities/individuals are often active at several institutions and therefore this system will enable banks and insurers to warn each other of these entities/individuals. The conditions are set out in the new Protocol Incident Warning System for Financial Institutions ("**PIFI**"). This protocol contains rules that banks and insurers must meet in order to keep track of and exchange data about incidents such as identity fraud or banking helpline fraud (otherwise known as 'spoofing').	20 August 2021	DDPA statement (in Dutch)

Development	Summary	Date	Links
	Financial institutions are allowed to maintain an overview of incidents within their own organization, including oversight of personal data. However, it is not permitted to exchange data on a large scale. The PIFI system includes a strict procedure for the exchange of data on a large scale. For example, if an institution takes on a new customer, it can only 'ask' other institutions whether that individual is properly registered. There will be no central database or blacklist in which to search for details of incidents. For each query, the institutions must consider whether it is necessary to provide or receive the personal data.		
Breach of the GDPR does not automatically imply impairment of the integrity of a person	On 25 June 2019, a Dutch local tax office for water authorities and municipalities sent a letter addressed to the claimant's former residential address. The office informed the claimant by email on 10 July 2019 that it had sent personal data to an incorrect address, as a result of which his personal data and other information had reached third parties. The claimant requested the office to rectify this and to demonstrate that his personal data had been destroyed. Following this e-mail, an e-mail exchange took place between the claimant and the office's data protection officer. During this e-mail exchange, it transpired that the claimant's e-mail address was sent to third parties and that one of these third parties had used his personal data for customer research purposes. The claimant argued that the processing of his personal data for customer research purposes was unlawful, because he had not given his consent and so consequently the office was not authorized to share his personal data for this purpose. The office reasoned that this processing was lawful, and that this processing was necessary for the performance of a task in the exercising of a public authority's role, as vested here in the office. Therefore no consent was required. The claimant requested the court to order the office to compensate him for the damages he had suffered as a result of the unlawful issuance of his personal data to third parties. Pursuant to Article 82(1) GDPR, any person who has suffered material or non-material damage as a result of a violation of the GDPR is entitled to receive compensation from the controller or processor. Pursuant to Article 82(2) GDPR, every controller	11 August 2021	Court ruling (in Dutch)

Development	Summary	Date	Links
	involved in processing is liable for the damages caused by processing data in violation of the GDPR. The court ruled that the claimant had not sufficiently demonstrated that he suffered material or non-material damage as a result of the disclosure of his personal data to third parties, either through the letter of 25 June 2019 or the sharing of his e-mail address with the third party for customer research purposes. The court was of the opinion that what happened was not a situation in which the adverse consequences of the (alleged) breach of standards were obvious. It did not concern such seriously culpable behavior that it must be qualified as a violation of a fundamental right. The court concluded that a violation of the GDPR does not automatically imply impairment of the integrity of an individual and therefore did not directly result in damages and compensation.		
DDPA publishes recommendations for smart cities	The DDPA has published recommendations for the development of so-called smart city applications. The recommendations are intended for municipalities that collect or plan to collect personal data in public spaces using smart sensors and measuring devices. The DDPA's recommendations are necessary because municipalities do not always pay sufficient attention to GDPR compliance in this regard. Poorly developed applications may impede the freedom of residents and visitors to that municipality, for example, they may be followed in public spaces in a way that is not necessary or not permitted. The DDPA has looked at the extent to which municipalities use smart city applications, both in terms of their implementation and development, and the extent to which these protect the personal data of residents and visitors. The range of smart city applications is significant, as whereas some municipalities are ahead in the development of smart city applications and deploying new technologies for this purpose, some municipalities are further behind and either use very few or no smart city applications. The DDPA drafted the following recommendations which should be followed by those who are developing, using or introducing smart city applications: – Ensure that the basic principles of the GDPR are followed.	30 July 2021	DDPA statement (in Dutch)

Development	Summary	Date	Links
	– The preparation of a DPIA for smart city applications is often mandatory, and munipalities should consider publishing the DPIA so that citizens are aware of how their privacy is guaranteed. – Draw up policies for the deployment of smart city applications and incorporate this into practical guidelines for implementation. – When procuring products and services, municipalities must conduct due diligence on whether they comply with the GDPR. – Research on how a local government can gain an insight into the sensors that are placed in public places by third parties and share this information with citizens. – Make sure there are enough people and resources to ensure privacy compliance within the municipality, and that any appointed data protection officer can fulfil their role properly. – Use the knowledge of citizens to map out the risks, given that they will know their own living environment best and can feed into the discussion about the consequences of a technical application.		
Social media video platform fined for violating children's privacy	The DDPA has imposed a fine of EU 750,000 on a social media video platform for violating the privacy of young children. The information the company's privacy statement that Dutch users – mostly young children – received when installing and using the app was in English and therefore was too difficult for children to comprehend. By not offering the privacy statement in Dutch, the company did not sufficiently explain how the application collects, processes and further uses personal data. Children are considered to be a vulnerable group under the GDPR and are given extra legal protection, given that they are generally less aware of the consequences of their actions, particularly the impact of the processing of their personal data by social media. Initially, the company had no head office in Europe and so the DDPA could not handle the investigation from the Netherlands, however, during the investigation the company then registered their office in Ireland. From that point, the DDPA was only authorised to rule on the company's privacy statement and therefore the Irish DPA will finalize the investigation and render a	22 July 2021	DDPA statement (in Dutch)

Development	Summary	Date	Links
	final judgment on other possible privacy violations that the DDPA has investigated. The DDPA handed its investigation findings to the company at the beginning of October 2020. The company subsequently promised and implemented various changes to make its app safer for children. For example, parents now have more control over their children's accounts on the platform, as they can manage their children's privacy settings through their own account and the app's Family Pairing function. The decision on the fine that will be payable by the company is not yet final, and the company has objected to any fine being imposed.		

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

Victor Mukhin
Associate
T: +7 812 363 3377
victor.mukhin@
eversheds-sutherland.ru

Mikhail Timonov
Partner
T: +7 812 363 3377
Mikhail.timonov@
eversheds-sutherland.ru

Ekaterina Zhevkova
Associate
T: +7 812 363 3377
ekaterina.zhevkova@
eversheds-sutherland.ru

Development	Summary	Date	Links
List of requirements for telecommunications operators is expanded	Numerous amendments have been made to the Law on Communications. Among other things, it establishes the requirement that only Russian legal entities may be the owners of communications lines which cross the national border of the Russian Federation. At the same time, the Law on Communications is supplemented by provisions stipulating the obligations of communications operators, owners of technological communication networks, owners of traffic exchange points and owners of communication lines which cross the national border of the Russian Federation. The amendments also stipulate the obligation of internet communications operators to provide free access to the sites and programs included in the list of socially significant domestic information resources. The list includes official sites of state bodies, local authorities, official sites of state non-budgetary	2 July 2021	Amendments to Federal Law on Communications

Development	Summary	Date	Links
	funds of the Russian Federation, portals of state and municipal services and other sites. The radio-frequency service is responsible for creating a system for ensuring the compliance of telecommunications operators with the established requirements. The amendments entered into force on 2 July 2021.		
Government to prepare new measures to support IT industry	The Russian Government has prepared an action plan in order to support the Russian IT industry, involving a range of measures which include increasing the demand for domestic IT solutions, ensuring accelerated digital transformation in the different economic sectors (as well as in the social sphere too), and creating the ideal environment for IT business to succeed in Russia. There are a number of measures that the Russian Government are proposing, with the key proposals being put forward as follows: – the removal of legislative restrictions and barriers to the use of modern digital solutions; – ensuring that there is a priority right of access to state support measures for IT companies in the field of information security; – financing the creation of Russian digital platforms with standard solutions for budgetary organisations; – the creation of conditions for the unimpeded use of existing tax incentives and support measures for the IT industry; and – the creation of an IT ombudsman institute to protect the IT companies' rights in order to identify systemic problems in the IT sector and work on complaints and appeals from individual entrepreneurs.	14 September 2021	Action Plan Road Map – Creation of additional conditions for the development of the information technology industry

Saudi Arabia

Contributors

Anmar Al Gharifi
Partner
T: +966 11 277 9820
anmaralgharifi@
aldhabaan-es.com

Muhammad Anum Saleem
Principal Associate
T: +966 11 277 9836
muhammadsaleem@
aldhabaan-es.com

Christine Khoury
Principal Associate
T: + 971 4 389 7064
christinekhoury@
eversheds-sutherland.com

Development	Summary	Date	Links
Saudi Data Protection Law 2021	On 24 September 2021, Saudi Arabia enacted its first comprehensive data protection law. It is also expected that the Regulations will provide further details on the implementation of the Personal Data Protection Law ("**PDPL**"). The PDPL applies to any processing of personal data related to individuals in the Kingdom by any means, including processing personal data related to individuals residing in the Kingdom from any party outside the Kingdom. The PDPL will come into effect on 23 March 2022, and the executive regulations supplementing the PDPL should also be issued within this period. The competent authority responsible for the implementation of the PDPL is the Saudi Data & Artificial Intelligence Authority known as "SDAIA". The PDPL states that the supervisory function will eventually shift to the National Data Management Office, which falls under SDAIA. In a nutshell, the PDPL is intended to (i) prohibit the processing of personal data without the owner's consent, except in specific circumstances, (ii) prevent that data from being misused by third parties (iii) ensure privacy of personal data, and (iv) regulate data sharing. In the event of a data breach incident, there is an obligation to notify the competent authority. Please read our full client briefing for further information.	24 September 2021	Eversheds Sutherland client briefing

Contributors

Singapore

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
Baseline testing framework for artificial intelligence governance	The Infocomm Media Development Authority ("**IMDA**") and the Personal Data Protection Commission ("**PDPC**") are working together to develop a credible minimum viable product ("**MVP**") testing framework for AI governance. This will allow organisations to deploy AI systems in a trusted manner as well as achieve greater transparency around the use of their AI systems. The MVP testing framework aims to help AI system owners and/or their developers to test and verify the performance of their AI solutions through a mix of technical and statistical tests and also process checks. Organisations with AI systems can expect internationally accepted AI ethics and governance principles to be translated into tangible results during the framework's verification process. The MVP testing framework identifies 12 ethical principles, which are sub-divided into the following 4 key aspects, which make up the foundations for a trustworthy AI system: – understanding how an AI model reaches a decision; – ensuring the safety and resilience of an AI system; – ensuring the AI system considers fairness in its decision making so that it does not unintentionally discriminate; and – ensuring management and oversight of an AI system. The cybersecurity and data governance of AI systems are also considered under the testing framework.	14 July 2021	PDPC's Developing the MVP for AI Governance Testing Framework

Development	Summary	Date	Links
Joint advisory on ALTDOS (a hacking group) by the Cyber Security Agency of Singapore, PDPC and Singapore Police Force	A joint advisory document (produced by the PDPC, Singapore Police Force and the Singapore Cyber Security Centre) has been issued to highlight the observed tactics, techniques and procedures employed by a threat actor group called "ALTDOS" to attack and compromise its victims' networks. ALTDOS first emerged in late 2020 and operates primarily in Southeast Asia and Bangladesh, targeting businesses for financial gains. Based on past incidents, it was identified that ALTDOS: – typically uses double extortion techniques to extract ransom from their victims; – exploits vulnerable web servers; and – employs default Cobalt Strike beacons as well using default Cobalt Strike TLS/SSL certificates. The joint advisory has provided some recommended measures for organisations to follow in order to mitigate the threat posed, for example: – performing regular patching of software to reduce any security vulnerabilities; – conducting regular log reviews in order to identify any malicious activities; – deploying network segregation or segmentation techniques so as to limit communications between internet facing services and internal servers; – implementing routine backups, which assist with system restoration thereby mitigating the impact of a ransomware incident and minimising data loss; – employing web application firewalls to filter malicious network traffic; and – seeking professional assistance to improve the organisation's overall cybersecurity.	24 August 2021	PDPC's Joint Advisory on ALTDOS

Development	Summary	Date	Links
PDPC's launch of a new application programming interface for the Do Not Call Registry	Organisations are generally prohibited under the Personal Data Protection Act 2012 from sending marketing messages to Singapore telephone numbers listed in the Do Not Call ("**DNC**") Registry, with the register being maintained by the PDPC. With the new API developed by the PDPC, organisations can now choose to connect their internal system with a new API system in order to check numbers in the DNC Registry. This avoids the risk of DNC infringements, with the API allowing organisations to check numbers in real time whilst the call is being made or when the text message is being sent.	1 September 2021	PDPC Do Not Call (DNC) Registry API for Existing DNC Registry Users document
Launch of the Better Data Driven Business (BDDB) programme	The IMDA and the PDPC have launched the BDDB programme in order to help small and mid-size enterprises ("**SMEs**") gain deeper consumer insights through the responsible use of collected data, therefore helping SMEs to scale up their businesses. The BDDB programme aims to support 2 types of SMEs: – those that are starting to learn to use data to generate insights; and – those that seek to apply and share data for more complex purposes. Developed with built-in basic data protection practices, organisations will be able to use the user-friendly business intelligence tool under the BDDB programme to generate insights from existing business data to address common business needs. These business needs can include awareness of growing product sales, acquiring new customers, retaining and engaging customers, improving human resources planning, and lowering inventory costs.	14 September 2021	Infocomm Media Development Authority's Better Data Driven Buinsess introduction page
PDPC's new guide and checklists for information comunications technology (ICT) systems	The PDPC has published a new guide comprising of a compilation of data protection practices from past PDPC advisory guidelines and guides. Besides drawing on lessons learnt from past data breaches, the new guide provides recommendations on basic and enhanced practices which organisations can incorporate into their ICT	14 September 2021	PDPC's Guide to Data Protection Practices for ICT Systems

Development	Summary	Date	Links
	policies, systems and processes in order to safeguard the personal data under their care. In the same guide, the PDPC has also compiled checklists to help organisations put in place and review any existing or new policies, technology controls and processes so as to avoid common mistakes that often result in data breaches.		
Revisions to PDPC guides to developing a data protection management programme and data protection impact assessments	The PDPC has updated its guide to developing a data protection management programme ("**DPMP**") so that it captures and incorporates best practices in accountability which will support organisations' personal data protection policies and processes. This also cover what a DPMP is and the importance of having one. The PDPC has also revised its guide to data protection impact assessments ("**DPIA**") to align with the new obligations under the updated Personal Data Protection Act 2012, which came into force on 1 February 2021. This covers the life cycle of a DPIA and when to conduct one, as well as who should be involved.	14 September 2021	PDPC's revised Guide to Developing a Data Protection Management Programme PDPC's revised Guide to Data Protection Impact Assessments
Industry consultation on the licensing framework for cybersecurity service providers	The Cybersecurity Act 2018 came into force on 31 August 2018 to establish a legal framework for the oversight and maintenance of national cybersecurity in Singapore. The Cybersecurity Act 2018 seeks to: (a) provide a framework for the regulation of critical information infrastructure; (b) provide the Cyber Security Agency of Singapore ("**CSA**") with powers to manage and respond to cybersecurity threats and incidents; (c) establish a framework for the sharing of cybersecurity information; and (d) establish a licensing framework for cybersecurity service providers. However, Part 5 of the Cybersecurity Act 2018 (which encapsulates the licensing framework) was deferred to allow for further study and consultation on the licensing framework in order to enhance its practicability for cybersecurity service providers. Generally, the licensing framework seeks to address three main considerations over time:	20 September 2021	CSA's Press Release

Development	Summary	Date	Links
	– providing greater assurance of security and safety to consumers; – improving the standards and standing of cybersecurity service providers; and – addressing the information asymmetry between consumers and the cybersecurity service providers. For a period of 4 weeks from 20 September 2021, the CSA sought industry feedback on its proposed licence conditions and draft subsidiary legislation under the licensing framework. Some of the key proposals by the CSA include: – imposing conduct requirements (such as maintaining confidentiality and not making false representations, etc.) for licensees to comply with in order to provide a baseline level of protection for consumers of cybersecurity services; – imposing requirements for licensees to provide information concerning or relating to their cybersecurity services in a timely manner upon CSA's request so that licensees may facilitate CSA's investigations, where applicable; and – imposing notification requirements under the Cybersecurity Act 2018 on organisations to notify the CSA of changes to information such as those relating to the honesty, integrity and financial soundness of such organisations so that the CSA may better assess the licensee's continued eligibility to be licensed. In the initial phase, the licensing requirements will apply only to those providing penetration testing and managed security operations centre monitoring services. It is expected that the licensing will be implemented by early 2022.		

South Africa

Contributors

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

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

Development	Summary	Date	Links
Commencement of the Protection of Personal Information Act 2013	The 12-month grace period which was granted to organisations within which to become compliant with the provisions of the Protection of Personal Information Act 2013 (Act No. 4 of 2013) ("**POPIA**"), expired on 30 June 2021. Accordingly, the provisions of POPIA became enforceable on 1 July 2021.	1 July 2021	
Notice regarding commencement date of section 58(2)	Section 57(1) of POPIA requires that a responsible party obtains prior authorisation from the Information Regulator in terms of section 58 if the responsible party plans to: – process any unique identifiers of data subjects: – for a purpose other than the one for which the identifier was specifically intended at collection; and – with the aim of linking the information together with information processed by other responsible parties; – process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties; – process information for the purposes of credit reporting; or – transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72. A responsible party must notify the Information Regulator of its intention to process personal information in accordance with section 57(1) of POPIA and may not carry out such processing	Date of notice: 1 July 2021 Adjusted commencement date of Section 58: 1 February 2022	Amendment to notice

Development	Summary	Date	Links
	that has been notified to the Information Regulator until the Information Regulator has completed its investigation. The Information Regulator has amended the commencement date of section 58, and has determined that the provisions of section 58 of POPIA will only be applicable from 1 February 2022.		
Guidance note on exemptions from the conditions for lawful processing of personal information	POPIA prescribes the eight conditions for the lawful processing of personal information by or for a responsible party. These conditions are not applicable to the processing of personal information to the extent that such processing is exempted, in terms of section 37 or 38, from one or more of the conditions concerned in relation to such processing. The Regulator has issued this Guidance Note to guide responsible parties who intend to apply for exemption from section 37 of POPIA, or who are exempt from complying with certain of the provisions of POPIA.	21 June 2021	Guidance Note on Exemptions from the Conditions of Lawful Processing Exemption Application Form
Guidance note on processing of special pesonal information	Section 26 of POPIA prohibits the processing of special personal information, subject to exceptions provided for in section 27(1). In terms of section 27(2) of POPIA, the Information Regulator may, subject to section 27(3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject. The Information Regulator has issued a Guidance Note to guide responsible parties who are required to obtain authorisation from the Regulator to process special personal information, as provided for in section 27(2) of POPIA.	21 June 2021	GUIDANCE NOTE ON PROCESSING OF SPECIAL PERSONAL INFORMATION
Information Regulator takes over PAIA functions from the South African Human Rights Commission	With effect from 30 June 2021, the Information Regulator has taken over the regulatory mandate function relating to the Promotion of Access to Information Act 2000 ("**PAIA**") which were previously performed by the South African Human Rights Commission. Some key objectives of the PAIA are to promote transparency, accountability and effective governance of all public and private bodies, as well as to assist members of the public to effectively	Date of notice: 21 June 2021 Publication of amendments: 29 July 2021	Media statement PAIA Manual Template for Public and Private Bodies Amended PAIA Regulations

Development	Summary	Date	Links
	scrutinise and participate in decision making by public bodies. PAIA ensures that the state promotes a human rights culture and social justice. It also encourages openness and it is there to establish mechanisms or procedures which give effect to the right of access to information in a speedy, inexpensive and easy manner. In relation to PAIA manuals, certain organisations were required to develop and publish PAIA manuals relating to the disclosure of information. The scope of information that the manual must cover has been widened to include matters relating to the processing of personal information in terms of POPIA. Up to now, an exemption has allowed smaller private bodies to be exempt from developing a manual. Effective from 1 January 2022, all public and private bodies (including those that are currently exempted) must have their PAIA Manual available at their principal place of business or on their website, if any, and from 30 June 2021, public and private bodies do not have to submit their PAIA Manual to the Regulator. In terms of sec 51(1) of PAIA, as amended, all previously developed PAIA manuals of both public and private bodies must be updated to include provisions relating to the processing of personal information in terms of POPIA. The Minister of Justice and Correctional Services has also published amendments to the Regulations applicable to PAIA, which amended the Regulations to place certain obligations on information officers to ensure that a copy of the responsible party's PAIA manual is available at their registered head office for public inspection during normal office hours.		
Invitation for public comments on the amendment of regulations relating to the protection of personal information	The Regulator has invited interested parties to submit written comments on the proposed draft regulations that amend the regulations issued under Section 112(2) of POPIA. Comments are to be submitted by 30 September 2021.	9 September 2021	Invitation for Comment Proposed Regulations

Switzerland

Contributors

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

Development	Summary	Date	Links
New EU Standard Contractual Clauses for cross-border data transfers can also be used in Switzerland	On 27 August 2021, the Federal Data Protection and Information Commissioner ("**FDPIC**") accredited the new Standard Contractual Clauses adopted by the European Commission on 4 June 2021, as a basis for cross-border transfers of personal data to countries without an adequate level of data protection from 27 September 2021 onwards. Existing cross-border data transfer agreements based on the old Standard Contractual Clauses or other model clauses (such as the Swiss Transborder Data Flow Agreement) remain valid until 31 December 2022, provided that there is no substantial change to the data transfer/processing underpinning the existing agreement or to the content of such agreement during this transitional period. The use of the new Standard Contractual Clauses for cross-border data transfers that are governed by the Swiss data protection law (in particular the Federal Act on Data Protection) requires some Swiss law specific adaptions and modifications, which can be included in an annex to the Standard Contractual Clauses. However, as is the case with transfers of personal data from the EU, the new Standard Contractual Clause will not always provide a sufficient data protection level to ensure a lawful cross-border data transfer. This is particularly the case if the data importer is subject to local laws and practices that are inconsistent with the data subjects' fundamental rights and freedoms. Controllers and processors who intend to transfer personal data to countries without an adequate level of data protection can therefore not simply rely on the new Standard Contractual Clauses, but have to carefully identify the risks related to the cross-border data transfer and to assess whether the Standard Contractual Clauses provide a sufficient level of protection for the data that is to be transferred or whether additional measures need to be and can be implemented. If such additional measures are not feasible, the controller or processor must refrain from transferring the personal data to the respective country.	27 August 2021	FDPIC statement Information sheet

United Kingdom

Contributors

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

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

Development	Summary	Date	Links
New DCMS guidance for tech companies on protecting users online	In May 2021, the government published a draft Online Safety Bill, which establishes a new regulatory regime and imposes a duty of care on online providers (that permit users to share user-generated content, and those that provide regulated search services) to protect its users from illegal and harmful content. On 29 June 2021, the Department for Digital, Culture, Media and Sport ("**DCMS**") published online safety guidance, aimed at helping tech companies owning or managing online platforms to protect their users from online harms such as child sexual exploitation and abuse, terrorist use of internet, hate crime and harassment, cyberbullying and online abuse. Its 'Safety by design' guidance is designed to assist companies enhance and prioritise the safety measures of their products to reduce the risk of online harm occurring. DCMS' 'one-stop shop' guide is the official government collection of guidance for online platforms on child safety.	29 June 2021	Press release Safety by design guidance One stop shop guide
NCSC's Cyber Security Toolkit for Boards hub	The National Cyber Security Centre ("**NCSC**") has published Cyber Security Toolkit for Boards hub, a collection of guidance and resources for Boards of directors aimed at encouraging and assisting discussions with technical cyber security experts. The toolkit covers nine standalone modules which focus on key topics in cyber security (including risk management for cyber security and how to implement appropriate cyber security measures) and is tailored specifically for Board members.	6 July 2021	Board toolkit hub NCSC blog Template questions for Boards

Development	Summary	Date	Links
	The NCSC has also created a supplementary document containing questions that Boards 'should be asking about cyber security'.		
ICO issues new detailed guidance on data protection and the EU following Brexit	The ICO updated its guidance on data transfers from and to the EU and the EEA. The updates reflect the adoption by the European Commission on 28 June 2021 of the adequacy decisions under the EU GDPR and the Law Enforcement Directive (EU) 2016/680, which allow the transfers of most personal data from the EU and the EEA to the UK without additional safeguards. The Data protection and the EU in detail guidance is aimed at Data Protection Officers and other persons with data protection responsibilities. It explains the implications of the adequacy decisions, and provides advice on international data transfers, EU and UK representatives, EU regulatory oversights and law enforcement processing.	7 July 2021	ICO updated guidance ICO guidance on LED ICO guidance on UK GDPR
ICO publishes 2020-2021 report and annual tracking research	On 7 July 2021, the ICO published its 2020-2021 annual report, outlining its six strategic 'goals' over the next year, including increasing the public's trust and confidence in how their data is used and made available, and ensuring that the ICO stays abreast of evolving technologies and industries. The report highlights the ICO's specific areas of focus for enforcement, including: investigating credit reference agencies, investigating the adtech industry, investigating the use of mobile phone extraction by police forces and acting against nuisance marketing firms (for which it issued fines totalling £2.306 million under PECR in 2020-2021). The ICO also published its annual tracking research, which monitors changes in public opinion relating to data protection. The research revealed that 77% of UK people consider protection of their personal information to be essential.	7 July 2021	Press release Annual report Annual tracking research
Government consults on Plan for Digital Regulation	On 6 July 2021, the Department for Digital, Culture, Media & Sport ("**DCMS**") published its policy paper entitled "Digital Regulation: Driving growth and unlocking innovation". The policy paper explores the issues surrounding encouraging the adoption of new digital technologies to drive innovation and	6 July 2021	DCMS policy paper Ten Tech Priorities

Development	Summary	Date	Links
	balancing the governance of such technologies. It sets out the DCMS' "Plan for Digital Regulation", which proposes how technology will be regulated in the UK in future. The Plan is centred around three strategic objectives: (i) promoting competition and innovation across the digital sector; (ii) keeping the UK safe and secure online; and (iii) promoting a flourishing democratic society. The Plan builds on the DCMS' Ten Tech Priorities, which include keeping the UK safe and secure online, fuelling a new era of startups and scaleups, and leading the global conversation on tech. The DCMS issued a call for views on the policy paper, to be submitted by 28 September 2021.		
Government launches online media literacy strategy	On 14 July 2021 the UK Government launched its Online Media Literacy Strategy. The objective of the strategy is to support organisations to undertake media literacy activity in a more coordinated, wide-reaching, and high quality way over the next 3 years – with the overall goal of improving media literacy capabilities for users across the UK. The strategy will support the objective in four ways: – setting out a strategic direction for the future of media literacy in the UK – ensuring a coordinated approach to media literacy activity – addressing key gaps within the media literacy landscape – reducing barriers and creating opportunities for organisations undertaking media literacy activity The strategy accompanies the new Online Safety Bill, which will establish a new duty of care to make companies take responsibility for the safety of their users and address harmful content.	14 July 2021	Policy paper
CDEI publishes beta version of Privacy Enhancing Technologies adoption guide	On 14 July, the Centre for Data Ethics and Innovation ("**CDEI**") published a beta version of its PETs adoption guide – an interactive tool created to help with decision making around the use of privacy enhancing technologies (PETs) in data driven projects. It is supported by a repository of real-world use-cases.	14 July 2021	CDEI blog post

Development	Summary	Date	Links
	The CDEI has been collecting feedback on the guide and conducting usability tests to maximise its relevance and usefulness to developers and practitioners.		
DCMS consults on digital identities regime	DCMS announced that it is running a consultation on digital identity and the governing body which will oversee the rules on digital identity (using digital means to prove identity without the use of physical documents). The consultation sought views on how the digital identity system should operate, including the setting up of a governing body and how that body should look. The consultation ran until on 13 September 2021.	19 July 2021	DCMS consultation page
ICO publishes AI and data protection risk toolkit	The ICO has published an AI and data protection risk toolkit, in order to address the challenges of compliance with data protection principles for AI systems, including security risks from their use and the potential for discrimination and bias in the data. The toolkit is based on and compliments the Guidance on AI and data protection as well as the ICO's guidance, with The Alan Turing Institute, on Explaining decisions made with AI. The toolkit sets out the common risks of using AI to process personal data and recommendations on best practice techniques for mitigating risks and demonstrating compliance. The toolkit is now in beta form following the release of the alpha version in March 2021. The next stage will involve testing the toolkit on live AI systems to provide case studies on its usefulness. The final version is planned to be released in December 2021.	20 July 2021	ICO blog post
CDEI reports on role of data intermediaries	The CDEI published a report on the role of data intermediaries in supporting responsible data sharing. The report is intended to support the government's National Data Strategy programme – in particular, the commitment to consider the role of data intermediaries in supporting responsible data sharing, and how the government can intervene to support their adoption. The report explores the roles of seven types of data intermediaries: (i) data trusts; (ii) data exchanges; (iii) personal information management systems; (iv) industrial data platforms; (v) data custodians; (vi) data cooperatives; and (vii) trusted third	22 July 2021	CDEI blog post

Development	Summary	Date	Links
	parties. The report also speculates on the types of data intermediaries that may exist in the future. It explores data access and sharing issues, guiding individuals and businesses on how to use data intermediaries, and how to analyse data access and sharing.		
DCMS and ICO call for views on amending incident reporting framework for digital service providers under NIS regulations	The DCMS called for views on updating the incident reporting thresholds for digital service providers in the Network and Information Systems legislation (the **"NIS Legislation"**). The NIS Legislation is aimed at enhancing the level of information security of organisations that provide essential services to the UK (eg energy, water, healthcare, transport and digital infrastructure). The proposed amendments to the NIS Legislation are: – to revoke Article 4 from the UK-retained version of the EC Implementing Regulation (which sets out the thresholds); and – to allow the ICO, as the competent authority for digital service providers, to set the reporting thresholds at a more appropriate and proportionate level for the UK through new guidance. The ICO, as the competent authority for digital service providers, consulted on the level of reporting thresholds. The ICO's consultation closed on 7 October 2021.	26 July 2021	DCMS call for views ICO call for views
ICO updates COVID-19 regulatory approach document	At the start of the COVID-19 pandemic, the ICO published a document setting out their regulatory approach during the pandemic. The ICO updated this document to reinforce the following points: – the ICO's commitment to take into account (and continue taking into account) the range of challenges faced by organisations regulated by the ICO; and – the importance and value of information rights (the document sets out the ICO's expectations of organisations, including eg being able to deal with complaints they receive	27 July 2021	ICO blog post

Development	Summary	Date	Links
	from members of the public and having robust recovery plans in place). The ICO will continue to provide updates on their regulatory approach (including updating their regulatory action policy later this year) in order to provide continued clarity to organisations, both during the pandemic and after.		
Updated Code of Practice on the Management of Records under section 46 FOIA 2000	On 15 July, DCMS published an updated Code of practice on the management of records under section 46 of the Freedom of Information Act 2000. The revised code provides guidance to relevant public authorities on the retention, management and destruction of records. The updates made to the code by the National Archives reflect the current digital working environment.	15 July 2021	https://www.gov.uk/government/publications/code-of-practice-on-the-management-of-records-issued-under-section-46-the-freedom-of-information-act-2000
DCMS sub-committee inquiry into Government's approach to tackling harmful online content	The DCMS Sub-Committee on Online Harms and Disinformation launched a new inquiry into the Government's approach to tackle harmful online content, as outlined in its draft Online Safety Bill. The draft legislation would require all social media sites and search engines to remove any content that could cause individual harm (for example, terrorist content, content relating to child sexual exploitation and abuse and content containing disinformation that could affect an individual). The sub-committee will look into how Government focus has shifted since the introduction of the "Online Safety Strategy Green Paper" in 2017, and will specifically look at concerns surrounding the definition of "harm" and whether it is too narrow. The sub-committee will also explore key absences in the draft Bill (for example, a general duty for tech companies to deal with reasonably foreseeable harms and a greater focus on transparency) before the draft Bill is decided. The inquiry will also look into how and where lessons can be learned from different international efforts (for example, in France, Germany and Australia) to regulate harmful online content in big tech. The sub-committee invited written submissions in response to their inquiry by 3 September 2021.	27 July 2021	Inquiry details

Development	Summary	Date	Links
ICO approves GlobalSign as UK's first qualified trust service provider	The Information Commissioner's Office ("**ICO**") announced its approval of GMO GlobalSign Limited as the UK's first qualified trust service provider ("**QTSP**") under the UK's eIDAS Regulations, which has been added to the UK's trusted list of trust service providers accordingly. The eIDAS Regulations set out rules for UK trust services and establish a legal framework for the provision and effect of such services, including electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication. Trust services help to ensure that electronic transactions (for example, electronic fund transfers) can happen securely and legally using mechanisms such as electronic signatures; they are obviously important to businesses, especially during the ongoing COVID-19 pandemic. To become a QTSP, an organisation has to undergo a conformity assessment to demonstrate they meet the requirements of the UK eIDAS Regulations; this assessment is then further checked by the ICO. GlobalSign is the first organisation to have successfully gone through this process and is now a QTSP in the UK for the following services: – Qualified certificates for electronic signatures; and – Qualified certificates for electronic seals.	27 July 2021	ICO blog post
DCMS releases second version of digital identity trust frameworks	The DCMS issued a new version of its digital identity trust framework for consultation, following feedback gathered from third part organisations. It new version is intended to replace the first version of the framework which was issued in February 2021. Updates to the framework include: – the addition of guidance on the process whereby organisations become certified against the trust framework. The framework indicates that the UK Accreditation Service ("**UKAS**") will assess eligibility for accreditation via the completion of service audits;	2 August 2021	Press release Policy paper Consultation

Development	Summary	Date	Links
	– guidance on best practice for organisations working together to provide a streamlined and consistent approach to verification. This includes advice on how organisations can describe data in the same format to enable different organisations to understand the method of identity verification used; – improvements to the definitions of the trust framework's roles so that they are easier to understand; and – refinements of rules on topics such as managing digital identify accounts. The consultation closed on 13 September 2021.		
High Court provides clarity on the causes of action in 'external attacker' cases	In **Warren v DSG Retail Ltd** [2021] EWHC 2168 (QB), the High Court confirmed that a "use" (or "positive action") is required in order for the torts of breach of confidence and misuse of private information to be actionable in an "external, criminal third-party attacker" context. The claim arose following a data breach at DSG Retail Ltd ("**DSG**") (Dixons Carphone) when it suffered a complex cyber-attack in 2017-2018. The claimant sought to bring an action against DSG in breach of confidence, misuse of private information, breach of the Data Protection Act 1998 ("**DPA**") and in the alternative, common law negligence. The Court struck out the claims for breach of confidence and misuse of private information, concluding that these were ill-founded as those causes of action did not impose a data security duty on DSG. The Court also found that the claim in negligence failed as damages for negligence were not established unless and until damage has been suffered by the claimant. The Court allowed the claim for breach of the DPA in relation to Data Protection Principle 7, which requires DSG to take "appropriate technical and organisational measures" against "unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data". The claim is currently stayed pending the outcome of DSG's appeal to the First-tier Tribunal in relation to the £500,000 monetary penalty notice issued by the Information Commissioner's Office ("**ICO**").	30 July 2021	Judgment

Development	Summary	Date	Links
	The penalty was issued under the old DPA regime, as the cyber-attack pre-dated the introduction of the GDPR. This development will be welcomed by organisations facing cybersecurity threats which continue to grow in sophistication, frequency and coverage, because it: (1) signals claimant firms to reconsider citing extraneous causes of action in claims for compensation where data protection rights have been infringed; and (2) may serve to dissuade claimants from bringing proceedings in the first place due to growing uncertainty around the recoverability of ATE premiums. An ancillary impact of the judgment relates to costs recovery. By way of reminder, after-the-event insurance premiums are recoverable in "publication and privacy proceedings". However, claims for breach of data protection legislation are not classed as publication and privacy proceedings, which has led to claims being brought in misuse of private information and breach of confidence to help secure the recovery of after-the-event premiums. So where the only viable cause of action is under the statutory data protection regime (which is looking increasingly likely given the judgment in Warren v DSG Retail Ltd), then after-the-event premiums will not form part of a successful claimant's recoverable costs, which may dissuade claimants from pursuing litigation.		
New ICO guidance on direct marketing in the public sector	On 4 August 2021, the ICO issued new Direct marketing and the public sector guidance that seeks to help those responsible for data protection in public sector organisations to understand when direct marketing rules apply to the public sector. The guidance covers: an explanation of what direct marketing is; criteria for deciding whether public sector promotions are classed as direct marketing; why it is important for the public sector to know if their promotions are classed as direct marketing; the lawful bases for processing personal data under UK GDPR; the right for individuals to object to their personal data being processed under UK GDPR; and what a public sector organisation should consider if they wish to send another organisation's promotions.	4 August 2021	Article Guidance

Development	Summary	Date	Links
	The guidance highlights the obligation of public sector organisations to be open and honest about what they intend to do with an individual's personal data in order to comply with the UK GDPR, including the right to be informed, regardless of whether a communication amounts to direct marketing.		
ICO calls for views on employment practices ahead of guidance refresh	On 12 August 2021 the ICO announced the launch of a consultation on data protection and employment practices (the "**Consultation**") with the aim that this will help the ICO review its existing employment guidance (eg the ICO's Employment Code). The proposed new guidance will seek to address the changes in data protection law and to reflect the changes in the way employers use technology (eg AI and machine learning) and interact with their staff. Input is being sought from relevant stakeholders, including employers, professional associations, those representing the interests of staff, recruitment agencies, employment dispute resolution bodies, workers, volunteers, and employees, as well as suppliers of employment technology solutions. Any interested parties can participate in the survey via the options on the ICO's website. The consultation closes on 21 October 2021.	12 August 2021	Call for views
ICO seeks views on international data transfer tools for UK transfers	On 11 August 2021 the ICO launched a public consultation on its draft international data transfer agreement ("**IDTA**"), transfer risk assessments and related guidance. The intention is that the IDTA will replace the old EU Standard Contractual Clauses for international data transfers from the UK to third countries that are no longer an appropriate safeguard. The IDTA will take into account the *Schrems II* judgment of 16 July 2020 of the Court of Justice of the European Union insofar as it relates to the UK GDPR. The ICO also issued a draft UK addendum that seeks to amend the new EU standard contractual clauses issued on 4 June 2021 by the European Commission so that they can in principle be used for transfers made under UK GDPR.	11 August 2021	Consultation Eversheds Sutherland client briefing and podcast

Development	Summary	Date	Links
	Any interested parties can respond to the consultation via the ICO's website. The consultation closed on 7 October 2021. Eversheds Sutherland also published a briefing on this update.		
DCMS paper on data foundations and AI adoption in UK private and third sectors	The DCMS published research on the extent of data foundations and AI adoption in the UK private and third sectors – which forms part of its National Data Strategy programme of work. The findings of the research showed that: – over 99% of the organisations surveyed recognised the importance of data to their success and growth; – the adoption of data foundations appears to be relatively widespread, although the level of adoption was lower in the third sector (i.e. organisations that are neither private nor public sector, such as charities) than in the private sector; – all organisations that claim to have a high AI adoption also have a high data foundations adoption, however not all organisations with a high data foundations adoption have a high AI adoption which suggests that data foundations are a necessary (though not sufficient) condition for AI adoption; – there are challenges and barriers to data foundations adoption (including lack of skilled personnel and lack of funding) that are likely to continue into the future; and – AI remains an emerging technology, although a majority (~66%) of organisations have either adopted or are planning to adopt the technology. According to the research, within the UK private sector, nearly all large organisations (~90%) have planned or already adopted AI, whereas only 48% of SMEs have.	16 August 2021	Research paper
UK's Surveillance Camera Commissioner consults on revised code of practice	The UK Government has consulted on proposed amendments to the Surveillance Camera Code of Practice to reflect recent changes in legislation (the "**Code of Practice**"). The Code of Practice provides guidance on the appropriate use of surveillance camera systems by local authorities and the police. It is its first revision since its introduction in 2013.	13 August 2021	Code of practice Grid of proposed amendments

Development	Summary	Date	Links
	The Government intends to lay the revised draft Code of Practice before Parliament in late autumn.		
ICO approves first UK GDPR certification scheme criteria for three new schemes	The ICO has approved the first new certification criteria under Article 42(5) of the UK GDPR for three schemes: one for ADISA (an organisation which is expert in IT asset disposal); and two for the Age Check Certification Scheme ("**ACCS**") – one relating to age assurance and one looking at children's online privacy. Certification was introduced under the UK GDPR to help organisations demonstrate compliance with data protection law and to promote transparency and inspire trust with users of their goods and services.	19 August 2021	Blog
DCMS announces post-Brexit "global data plans" including preferred candidate for new Information Commissioner	On 26 August 2021, the Department for Digital, Cultural, Media & Sport ("**DCMS**") announced a package of post-Brexit global data plans, aimed at boosting growth, increasing trade and improving healthcare. The plans include: – the intention to form a multi-billion pound global "data adequacy" partnerships with the US, Australia and Republic of Korea. Future partnerships are also being prioritised with India, Brazil, Kenya and Indonesia. A mission statement on the UK's approach to international data transfers along with the UK manual for undertaking adequacy assessments, guidance for the UK manual and a map illustrating priority countries, were also published which are intended to be used to inform the assessment of an intended partner's commitment to high data protection standards. – John Edwards, named as the preferred candidate new Information Commissioner. Mr Edwards subsequently appeared before MPs on the DCMS Committee for pre-appointment scrutiny on 9 September 2021. – expanding the Information Commissioner's powers, enabling them to promote the responsible use of personal data to stimulate economic growth and innovation. – the launch of a new International Data Transfers Expert Council, a subgroup of the National Data Strategy Forum, to	26 August 2021	Press release (global data plans)

Development	Summary	Date	Links
	provide independent and expert advice, of both a technical and tactical nature, which will enable the government to deliver on its mission to champion the international flow of data. The proposals also included a consultation on the future of the UK's data protection legal regime, with the aim of making the regime more "ambitious, pro-growth and innovation-friendly" whilst maintaining secure and trustworthy privacy standards. See more on this below.		
ICO responds to proposal for Artificial Intelligence Act	The ICO provided its response to the European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the Artificial Intelligence Act ("**AIA**")). The ICO supports the push for providing an AI framework that is consistent and certain and serves the public interest but also acknowledges that AI brings with it certain data protection risks such as non-compliance with the GDPR's data minimisation principle. The ICO supports a number of points in the AIA proposal. The ICO are particularly interested in the Commissions' approach to two aspects of AI regulation: – the rights that individuals and groups have in relation to AI systems and how these rights can be exercised; – the effectiveness of the control and oversight measures suggested and the scope for auditing. The ICO has therefore requested clarity on: – how existing provisions (such as the provisions in data protection law that allow individuals to contest certain AI-driven decisions or to seek explanation of the decisions) will interact with the AIA; – the results of the approach used by the Commission which focusses on self-reporting and internal controls; – how the roles of the AIA's user/provider map onto the processor/controller responsibilities of the GDPR;	6 August 2021	ICO response to consultation

Development	Summary	Date	Links
	– how harmonised standards that enable AI providers to report compliance with AIA progress.		
DBEIS Regulatory Horizons Council publishes report on future of technological innovations and role of regulation	The Regulatory Horizons Council (an independent expert committee overseen by the Department for Business, Energy and Industrial Strategy), published a report: The future of technological innovations and the role of regulation. The paper comprises opinions on the future socio-economic context within which technological innovations will be delivered from 2021 to 2030 including: – how innovations might shape that content; – what could be done to bring about a preferred future; and – how regulation can act as an enabler. The report is made up of two parts. The first part covers the strategic issues raised by those interviewed, and the Regulatory Horizons Council offers its own input too. The second part focuses on the interviewees' commentary on various specific areas of technology. The report is not a recommendation report with no government response expected on its contents.	19 August 2021	DBEIS report
ICO calls on G7 to rethink cookie consent pop-ups	The ICO has called on the G7 to protect people's privacy more meaningfully by overhauling cookie consent pop-ups. The Information Commissioner noted that at present the temptation for most users is to automatically select "I agree" when they see a cookie pop-up. The Information Commissioner has presented ideas to the G7 on how to improve the cookie consent mechanism for stronger data protection. In order to respect personal privacy preferences and minimise use of personal data this proposal includes allowing people to set more permanent privacy preferences of their choosing in web browsers, software application and device settings so that they do not have to do so via pop-ups each time they go to a website.	7 September 2021	ICO press release
ICO publishes enforcement notice for contravention of Article 15 of both the EU and UK GDPR	The ICO has published an enforcement notice against First Choice Selection Services Ltd ('First Choice') due to a failure by them to inform a data subject about whether their personal data was being processed by or on behalf of the controller alongside failing	7 September 2021	Enforcement notice ICO link to enforcement notice

Development	Summary	Date	Links
	to provide access to this personal data without undue delay which contravenes Article 15 of both the UK and EU GDPRs. The enforcement notice requires First Choice to provide a suitable response to the subject access request and also to review and update its internal systems, procedures and policies so that any future requests are dealt with properly. This is a reminder to all organisations in all sectors about the importance of dealing with rights requests from data subjects. The exercise of rights is a fundamental component of the UK and EU GDPRs. The individual concerned was in the process of bringing an employment tribunal claim and had made a subject access request which First Choice failed to respond to. If First Choice fail to comply with the enforcement notice then the Commissioner may serve a penalty notice of an amount up to £17,500,000 or 4% of total annual worldwide turnover (whichever is higher).		
ICO launches consultation on reporting thresholds under the NIS Regulations	The UK Government intends to amend incident reporting thresholds for digital service providers under the NIS Regulations 2018. The incident reporting thresholds are currently set out in EU retained law but do not work for the UK as they are set on the basis of EU market size. It is intended that the incident reporting thresholds will be moved from legislation into ICO guidance. The ICO, as the competent authority for digital service providers, is now consulting on the level of reporting thresholds. The consultation closes on 7 October 2021.	9 September 2021	
DCMS launches consultation on reforms to UK data protection and ePrivacy regime	On 9 September 2021 the Department for Digital, Culture, Media & Sport (the "**DCMS**") announced the Government's plans to reform the UK's data protection laws. On the following day, the DCMS opened a consultation on these changes. The reforms are a part of the government's National Data Strategy and shaping of a new UK data protection regime that will uphold a high standard of data protection and public	9 September 2021	Data: a new direction – consultation Press Release

Development	Summary	Date	Links
	trust, without needless burdens for business or barriers to innovation and international data transfers. The DCMS has also broadcasted proposed reforms to the ICO, which entail stricter penalties for nuisance calls and text messages and the creation of an independent board and Chief Executive. The DCMS' public consultation closes on 19 November 2021.		
ICO blog post contains guidance for universities and colleges on use of personal data in an emergency	On 14 September 2021 the ICO published a blog post containing guidance for universities and colleges in relation to handling sensitive personal data about students. The post is in response to a hesitation by universities and colleges to share personal data in urgent or emergent situations, out of concern that data protection laws will not allow it. The ICO has clarified that staff at these institutions must act in a way that is necessary and proportionate "to protect someone's life", which may include sharing an individual's personal data when it is required to prevent loss of life or serious harm (physical, emotional or mental). The ICO has added that there is no intention to penalise organisations who have acted in good faith and that they will take a pragmatic and proportionate approach when reviewing the sharing of personal data. The ICO has also set out four practical steps for universities and colleges to take to prepare for situations where personal data may need to be shared, and to help staff gain confidence and knowledge in this area, so that they know how to act in an emergency. These are: – have an emergency plan in place for crisis scenarios which includes guidance on sharing personal data; – have a data sharing agreement in place to ensure that information is shared safely and timely; – give staff training on how to use and share personal data and including specific training relating to emergency situations; and	14 September 2021	Blog: Sharing personal data in an emergency – a guide for universities and colleges | ICO Data sharing code of practice Data sharing information hub

Development	Summary	Date	Links
	– share access to the ICO's resources, including the data sharing code of practice and data sharing information hub. The ICO will continue working with universities, educational bodies and parents in this area, to provide reassurance that data protection law does enable the sharing of personal data "to save lives and protect young people".		
ICO publishes list of organisations eligible for BCRs	On 20 September 2021 the ICO published an update to the Binding Corporate Rules ("**BCRs**") which it had previously authorised under Article 26(2) of Directive 95/46/EC (the "**Directive**"). The ICO issued authorisation to holders of EU BCRs under the Directive, who were automatically eligible for a UK BCR, under the Data Protection Act 2018 ("**DPA 2018**"). These organisations have been permitted to rely on a UK BCR as a valid transfer tool since 1 January 2021. The ICO has now published a list of the organisations who were automatically entitled to a UK BCR under the DPA 2018, and who have affirmed that they seek a UK BCR. Organisations who are eligible and seeking a UK BCR, but have not been included on the list should contact the ICO immediately at BCR@ico.org.uk	22 September 2021	Binding Corporate Rules
Government launches annual cyber security breaches survey	The Department for Digital, Culture, Media and Sport (**DCMS**) has confirmed that the annual survey on cyber security breaches is set to be carried out between October 2021 and February 2022. The survey is aimed at UK businesses, educational institutions and charities' approach to cyber security and any challenges they face in this area, and the research will inform government policy in relation to cyber security. Ipsos MORI will carry out the fieldwork this year (which will consist of telephone interviews lasting approx. 20 minutes) and participation in the survey is voluntary and confidential.	27 September 2021	Survey

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

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

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

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

Development	Summary	Date	Links
New ransomware guidance from the New York Department of Financial Services	The New York Department of Financial Services ("**NYDFS**") recently released ransomware guidance. Citing the increasing number of ransomware attacks, NYDFS warned that a ransomware attack on multiple financial services companies at the same time could lead to a loss of confidence in the financial system. The guidance describes nine security controls for preventing and responding to cybersecurity incidents that NYDFS expects regulated companies to implement whenever possible. The security controls are: – Email Filtering and Anti-Phishing Training; – Vulnerability/Patch Management; – Multi-Factor Authentication; – Disabling Remote Desktop Protocols Access;	30 June 2021	NYDFS Guidance

Development	Summary	Date	Links
	– Password Management; – Privileged Access Management; – Monitoring and Response; – Testing and Segregated Backups; – Incident Response Plan. The guidance also notes that NYDFS is continuing to evaluate what additional controls should be added to existing Cybersecurity Regulations and encourages engagement by industry stakeholders and experts on future controls.		
Financial Crimes Enforcement Network makes cybercrime a priority	The Financial Crimes Enforcement Network ("**FinCEN**") provided an update on implementation of the Anti-Money Laundering Act 2020 ("**AML Act**") and issued the first government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy (Priorities). The Priorities, released on the AML Act's six-month anniversary, identify and describe the most significant AML/CFT threats in FinCEN's view. FinCEN picked eight priorities, including cybercrime. The update also noted that, as required by Section 6305(a) of the AML Act, FinCEN presented its assessment to Congress on 28 June 2021 regarding whether it would be helpful to establish a process by which FinCEN could issue "no-action letters." Establishing a process for no-action letters would allow an entity to submit an inquiry about how the BSA and other AML laws would apply in a particular situation. In addition to providing comfort to the submitting party, FinCEN also would be able to communicate its stance on practical applications of the AML laws to the public.	30 June 2021	FinCEN AML Update
Connecticut creates cybersecurity safe harbour	Connecticut adopted a cybersecurity statutory safe harbour on 6 July 2021. The law recognizes that cybersecurity attacks have become increasingly prevalent and incentivises businesses to implement cybersecurity safeguards. The safe harbour prohibits Connecticut courts from assessing punitive damages against a defendant in a tort action if the defendant has complied with an industry-recognized cybersecurity framework. The law includes several industry standards that would satisfy the requirement,	6 July 2021	Text of the Connecticut Safe harbour

Development	Summary	Date	Links
	including National Institute of Standards and Technology ("**NIST**") "Framework for Improving Critical Infrastructure Cybersecurity," NIST SP 800-171, NIST SP 800-53, and the ISO/IEC 27000 series. The law will go into effect 1 October 2021.		
California AG develops online tool for CCPA enforcement	After one year of the California Consumer Privacy Act ("**CCPA**") enforcement, the California Attorney General's office has released an online tool for consumers to report alleged violations of the CCPA. The online tool currently is limited to reporting businesses who do not post a "Do Not Sell My Personal Information" link on their websites. The tool asks users guided questions to determine whether the business has violated the CCPA. The tool will then generate an email for the user to send to the business to notify it of the non-compliance. These emails could have important ramifications for future Attorney General enforcement actions. The Attorney General can only sue businesses for CCPA violations after giving the business 30 days to cure any violations from the date of notification. Typically, it is the date of notification corresponding to the date on the letter of noncompliance; but going forward, the Attorney General could consider the clock to start upon generation of the email from the online tool. While consumers can currently only use the tool to report websites without "Do Not Sell My Personal Information" links, the Attorney General's office might update the tool in the future to allow users draft non-compliance emails for a wide variety of CCPA violations.	17 July 2021	CCPA Consumer Privacy Tool
FTC settles with colouring book app over COPPA violations	The Federal Trade Commission recently announced a settlement with a company operating a colouring book app, and its subsidiaries. The FTC alleged the app violated the Children's Online Privacy Protection Act Rule (COPPA Rule). Under the COPPA Rule, if any part of a website or app is directed at children under 13, the website or app must notify parents and obtain verifiable parental consent before collecting any information from the children. Though the app is primarily marketed toward adults, a portion of the app contains content specifically geared towards children. The FTC alleged that the app collected personal information from children without obtaining parental consent and	21 July 2021	Settlement Order

Development	Summary	Date	Links
	allowed third-party advertisers to collect personal information from the children for targeted ads. The settlement requires the company to take steps to remedy the COPPA Rule violations. The company must notify users of the alleged violations, delete all personal information collected from children unless it can obtain parental consent, offer a refund to current paid subscribers who are or were under the of 18 at the time of registration and pay a monetary penalty.		
CISA collaborates with US government agencies, the UK, and Australia to release joint cybersecurity advisories	Recognising the importance of international collaboration, the Cybersecurity and Infrastructure Security Agency ("**CISA**") released two joint cybersecurity advisories this quarter. CISA collaborated with the Australia Cybersecurity Centre, the United Kingdom's National Cyber Security Centre and the Federal Bureau of Investigations ("**FBI**") to release an advisory that highlights the top Common Vulnerabilities and Exposures ("**CVE**") routinely used by cyber actors in 2020 and sheds light on what CVEs are being exploited so far in 2021. The advisory recommends organizations apply "patches" to 30 identified vulnerabilities and implement a centralised patch management system. On 22 September 2021, CISA, the FBI and the National Security Agency ("**NSA**") published another advisory. The advisory specifically concerns increased Conti ransomware cyberattacks and includes steps organisations can take to counteract and mitigate the risk of Conti ransomware. The advisory explains that CISA and the FBI have combined observed over 400 instances of Conti ransomware attacks on organizations. The advisory recommends all companies take specific steps to mitigate the risk of Conti ransomware attacks.	CVE Advisory: 28 July 2021 Conti Ransomware Advisory: 22 September 2021	CVE Advisory Conti Ransomware Advisory
California District Court dismisses closely watched Communications Decency Act case	The U.S. District Court for the Northern District of California has dismissed all of the claims against Malwarebytes Inc. in *Enigma Software Group USA LLC v. Malwarebytes, Inc.* The parties are both anti-malware software companies. Enigma brought a claim against Malwarebytes, alleging that Malwarebytes violated various state laws by flagging some of Enigma's anti-malware software on consumer's computers as potential unwanted programs. Malwarebytes argued it was immune from these claims under Section 230 of the Communications Decency Act 1996.	9 August 2021	District Court Order

Development	Summary	Date	Links
	Section 230 provides, among other things, protections for providers of computer services who take actions in good faith to restrict access or availability to material that the provider considers to be objectionable. The district court found that Malwarebytes was entitled to the protection of Section 230 and granted its motion to dismiss. The Ninth Circuit reversed, finding that Section 230 did not allow software companies to filter out content for anti-competitive reasons. The Ninth Circuit remanded for further proceedings to determine whether Malwarebytes flagged Enigma's content for anti-competitive reasons. On 9 August 2021, the district court dismissed all of the claims without deciding whether Malwarebytes was protected by Section 230. The court found that Enigma had not adequately shown that Malwarebytes violated either of the state laws or acted in a tortious way. While the court did not rule on Section 230, the Ninth Circuit's opinion leaves open the question of when a provider acts for "anti-competitive" reasons, thereby losing the protection of Section 230.		
FINRA releases paper on cloud computing for securities brokers-dealers	The Financial Industry Regulatory Authority ("**FINRA**") released a paper on cloud computing in the securities industry. FINRA reminded broker-dealers that any shift to cloud computing must comply with regulatory requirements, such as ensuring the security and confidentiality of customer records and information, protecting against anticipated threats or hazards to customer information, protecting against unauthorized access to customer records that could result in substantial harm or inconvenience and preserving customer records for the period required by regulations. The paper emphasised that any firm adopting cloud computing should consider cybersecurity, data governance, outsourcing/vendor management, business continuity and record keeping. The paper also warned firms that after adopting cloud computing, the firm must supervise the cloud service provider to ensure customer information remains secure.	16 August 2021	FINRA Paper
SEC settles with alternative data provider amid intensified scrutiny on cybersecurity	The Securities and Exchange Commission ("**SEC**") recently announced a $10,000,000 settlement with App Annie, Inc., an alternative data provider for the mobile app industry. App Annie	Sanctions Against Broker-Dealers: 30 August 2021	SEC's Announcement of Broker-Dealer Sanctions

Development	Summary	Date	Links
	misused non-aggregated and anonymised confidential data received from mobile apps to alter some of the company's models in an attempt to make the model's estimates more valuable to trading firms. The trading firms then relied on the estimates to make investment decisions. The SEC found that App Annie engaged in deceptive conduct and made material representations in violation of security laws. This settlement comes after the SEC announced sanctions against several broker-dealer firms. The SEC sanctioned several brokers-dealers in August for violating Regulation S-P by failing to protect confidential customer information. Each of the firms sanctioned failed to adopt adequate cybersecurity policies, resulting in email account takeovers exposing personal information of thousands of customers.	Settlement with App Annie: 14 September 2021	SEC's Announcement of the App Annie Settlement
OFAC sanctions virtual currency exchange and updates ransomware advisory	The US Department of the Treasury Office of Foreign Assets Control ("**OFAC**") has for the first time designated a virtual currency exchange, SUEX OTC, S.R.O. ("**SUEX**"), on the Specially Designated Nationals and Blocked Persons ("**SDN**") List for its role in facilitating financial transactions involving illicit proceeds from at least eight ransomware variants. According to OFAC, SUEX's transaction history showed that over 40% of the exchange's transactions is associated with illicit actors. As a result of the SDN designation of SUEX, any company paying ransomware through the SUEX exchange is now violating sanctions regulations and is subject to civil or criminal penalties. OFAC also issued an updated ransomware advisory, which included more discussion on virtual currencies and guidance on defensive and response measures to take in the event of a ransomware attack. Such defensive measures include those highlighted in the US Department of Defense Cybersecurity and Infrastructure Security Agency's September 2020 Ransomware Guide, like maintaining offline backups of data, developing incident response plans and instituting cybersecurity training, among others. OFAC noted that it would view taking such steps, along with self-reporting ransomware attacks to law enforcement, as a mitigating factor in any OFAC enforcement response to a ransomware payment.	21 September 2021	OFAC Press Release OFAC Updated Advisory

For further information, please contact:

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

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

@ESPrivacyLaw

Editorial team

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

Ruth Haynes
Trainee Solicitor
T: + 44 20 7919 0599
ruthhaynes@eversheds-sutherland.us

Thomas Holt
Trainee Solicitor
T: + 44 121 232 1360
thomasholt@eversheds-sutherland.com

Leighann Mountain
Trainee Solicitor
T: + 44 1473 284 530
leighannmountain@eversheds-sutherland.com

Lauren Pettit
Trainee Solicitor
T: + 44 1223 44 3831
laurenpettit@eversheds-sutherland.com

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

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

eversheds-sutherland.com

CAM_1B\7547480\2