



Update

Your quarterly Data Privacy and
Cybersecurity update

July to September 2019



Executive summary



Welcome to the fifth edition of Udata!

Udata is an international update 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 2019 and is packed full of interesting news items from our contributors around the globe, including:

- [new guidelines from the European Commission on Ethics in AI](#);
- [the CNIL's guidelines on cookies and trackers](#);
- [guidance in Germany for financial services organisations on outsourcing to cloud service providers](#);
- [news of Latvia's first significant GDPR fine](#);
- [a new certification scheme in the Netherlands](#); and
- a number of developments in [China](#), including a new Cryptography Law and Regulations on Cyber Protection of the Personal Data of Children.

You can also read our [Spotlight On...](#) briefings, which provide more in-depth analysis of particular topics, such as our briefings on the CJEU's ruling relating to social media plugins and joint controllership and Operational Resiliency for Financial Institutions.

At the time of publication, we have been hit by a wave of new developments. We have referenced our recent briefings on the [CJEU's ruling that pre-ticked boxes are not sufficient consent for cookie placement](#) and the [UK Court of Appeal's decision to allow a data protection representative claim to proceed](#) for your information.

We have included a summary of the latest developments in relation to the [California Consumer Privacy Act 2018](#).

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

Jump to your region of interest

General EU and
International

Austria

Romania

France

Switzerland

Germany

United Kingdom

Hungary

China

Ireland

Hong Kong

Italy

Malaysia

Latvia

Mauritius

Lithuania

South Africa

Netherlands

United States

Poland

Russian Federation

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
World Economic Forum "Incentivising responsible and secure innovation" report	<p>The World Economic Forum's ("WEF") report "Incentivising responsible and secure innovation" focuses on why and how investors in technology-driven companies should embed cyber risk management and cybersecurity into their investment decisions.</p> <p>The WEF suggests that by ensuring cybersecurity from the outset – including features like security-by-design and security-by-default – investors can increase the likelihood of company success in the long term, promote more durable technology and improve overall cyber resilience.</p> <p>The report includes commentary around the need for greater awareness and a standard approach, the development of a cybersecurity due diligence framework, and new incentive structures to facilitate a balance between time to market and improved security.</p>	3 July 2019	WEF report Press release
EDPB twelfth plenary 9-10 July	<p>The European Data Protection Board ("EDPB") convened for their twelfth plenary on 9-10 July. Following the meeting, the EDPB published the following:</p> <ul style="list-style-type: none"> – Draft video surveillance guidelines; – EPDB-EDPS joint response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection; – Opinion on Standard Contractual Clauses for processors under Article 28(8) submitted by the Danish supervisory authority; 	9-10 July 2019	EDPB agenda Draft video surveillance guidelines EPDB-EDPS joint response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection and Annex



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – Opinion on draft accreditation requirements for a code of conduct monitoring body pursuant to Article 41 GDPR submitted by the Austrian supervisory authority; – Opinion on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment; – Joint Opinion on processing of patients' data and role of European Commission within eHealth Digital Services Infrastructure; – Opinion on the draft DPIA list of the Cyprus supervisory authority pursuant to Article 35(4); – Opinions on Art 35.5 lists (DPIA exemption) submitted by France, Spain and the Czech Republic; and – Recommendation on EDPS list pursuant to Art 39.4 Regulation 2018/1725 (DPIA list). 		Opinion on Danish DPA Art 28(8) SCCs Opinion on Austrian DPA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR Opinion on the competence of a supervisory authority in case of change in circumstances relating to main or single establishment Joint Opinion on processing of patients' data and role of European Commission within eHealth Digital Services Infrastructure Opinion on the draft DPIA list of the Cyprus supervisory authority pursuant to Article 35(4) Opinions on Art 35.5 lists (DPIA exemption) submitted to the Board by France , Spain and the Czech Republic Recommendation on EDPS list
European Insurance and Occupational Pension Authority consultation on cloud outsourcing	The European Insurance and Occupational Pension Authority ("EIOPA") has launched a consultation on guidelines on outsourcing to cloud service providers. The guidelines will provide advice to market participants on how the outsourcing provisions	1 July 2019	EIOPA press statement Consultation paper



Development	Summary	Date	Links
	<p>of the Solvency II Directive 2009/138/EC, Commission Delegated Regulation (EU) 2015/35 and EIOPA's Guidelines on System of Governance need to be applied in relation to outsourcing to cloud service providers. The consultation will close on 30 September 2019.</p> <p>The guidelines cover the following:</p> <ul style="list-style-type: none"> – criteria to distinguish whether cloud services should be considered within the scope of outsourcing; – principles and elements of governance of cloud outsourcing including documentation requirements and list of information part of the notification to supervisory authorities; – pre-outsourcing analysis, including materiality assessment, risk assessment and due diligence on the service providers; – contractual requirements; – management of access and audit rights; security of data and systems; sub-outsourcing, monitoring and oversight of cloud outsourcing and exit strategies; and – principle based instructions for the national supervisory authorities on the supervision of cloud outsourcing arrangements including, where applicable, at group level. 		
FSB launches survey on response to and recovery from cyber incidents	<p>The Financial Stability Board ("FSB") launched a survey of industry practices in the financial and non-financial industry sectors on response to, and recovery from, cyber incidents. Responses are requested by 28 August 2019.</p> <p>The FSB is developing a toolkit of effective practices to support financial institutions in their cyber response and recovery efforts. The survey aims to collect information on industry practices from industry on response and recovery of critical services, including restoration of data integrity following a cyber incident that could have an impact on financial stability.</p> <p>The FSB notes that the survey is a key element of the FSB's outreach strategy with external stakeholders to gather views on effective practices relating to financial institutions' response to, and recovery from, a cyber incident. The development of the</p>	11 July 2019	Press statement Survey



Development	Summary	Date	Links
	<p>toolkit will also be informed by a review of publicly available documents on how firms have responded to and recovered from past cyber incidents, and a stocktake of relevant publicly released guidance issued by national authorities and international organisations.</p>		
Europol and Eurojust “Common challenges in combating cybercrime” report	<p>Europol and Eurojust published a report summarising the key developments and challenges in combating cybercrime from both a law enforcement and a judicial perspective. The report is informed by operational and practical experience, joint deliberations and expert input. It identifies five key areas of focus (as noted in the press release):</p> <ul style="list-style-type: none"> – Loss of data: electronic data is the key to successful investigations in all the cybercrime areas, but the possibilities to obtain such data have been significantly limited. – Loss of location: recent trends have led to a situation in which law enforcement may no longer establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. – Challenges associated with national legal frameworks: the differences in domestic legal frameworks in EU Member States often prove to be serious impediments to international cybercrime investigations. – Obstacles to international cooperation: in an international context, no common legal framework exists for the expedited sharing of evidence (as does exist for the preservation of evidence). There is also a clear need for a better mechanism for cross-border communication and the swift exchange of information. – Challenges of public-private partnerships: cooperation with the private sector is vital for combating cybercrime, yet no standardised rules of engagement are in place, and investigations can thus be hampered. 	5 July 2019	Report Press release
European Commission reflects on GDPR implementation and refers Greece and Spain to the Court for not transposing	<p>In a report entitled “Data protection rules as a trust-enabler in the EU and beyond – taking stock”, the European Commission reflects on the GDPR’s first year of implementation and sets out</p>	24 July 2019	Report and accompanying press release



Development	Summary	Date	Links
Data Protection Law Enforcement Directive	<p>steps to strengthen the data protection rules and their application. The report concludes that most Member States have set up the legal framework required by the GDPR, and that the new system of strengthening the enforcement of data protection rights and rules is falling into place. Organisations are developing a compliance culture, citizens are becoming more aware of their rights and convergence towards high international data protection standards is progressing.</p> <p>In addition, the European Commission has referred Greece and Spain to the Court of Justice of the EU for failing to transpose the Data Protection Law Enforcement Directive, which was required to be transposed into national law by 6 May 2018.</p>		Press release (Greece and Spain)
CJEU rules that website operator can be joint controller in respect of personal data transmitted via social plugin	<p>In Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, the Court of Justice for the European Union has ruled that the operator of a website that features a Facebook “Like” button can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of personal data of visitors to its website. However, the website operator cannot be considered to be a controller in respect of the operations involving data processing carried out by Facebook after that data has been transmitted.</p> <p>The Court further confirmed that, as a joint controller, the website operator is required to comply with its data protection compliance responsibilities, including (among others): to provide specific information to the individuals whose personal data is being processed, and to ensure that it has a lawful basis for the processing that it is jointly determining occurs.</p> <p>The background is that a German clothes retailer embedded a Facebook “Like” button on its website, which facilitated the transmission of the website visitor’s personal data to Facebook Ireland. The transmission occurred as a result of the website including the button, without the visitor being aware of the transmission, and regardless of whether the visitor was a member of Facebook or had clicked on the “Like” button. A German consumer protection group brought an action against the retailer in 2015, citing that Fashion ID had failed to comply with</p>	29 July 2019	Press release Judgment Eversheds Sutherland briefing



Development	Summary	Date	Links
	<p>certain requirements under the former Data Protection Directive 95/46/EC.</p> <p>This case concerned the Facebook “Like” button but the judgment applies to other social media plugin technologies. Organisations should consider auditing their websites to ensure that they are deploying social media plugin technology in a compliant manner.</p> <p>You can read our briefing here.</p>		
ISO/IEC 27701:2019 Security techniques	<p>The International Organization for Standardization (“ISO”) and the International Electrotechnical Commission (“IEC”) and has published the first international standards for privacy information management. The standard specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to existing standards ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.</p>	22 August 2019	Standard description Standard foreword, introduction and table of contents
Recommendations to G7 Leaders on how to promote innovation, digital technology and trade	<p>The Information Technology Industry Council along with global tech industry groups have produced recommendations for G7 member countries regarding digital technologies, trade, and innovation. The recommendations encourage that the G7: reach an early agreement on the World Trade Organization Joint Statement Initiative on E-Commerce, facilitate the free flow of data across borders, increase the levels of privacy protection, support development of AI standards, enhance cybersecurity through global best practices and oppose measures that force disclosure of any sensitive information as a condition of doing business.</p>	22 August 2019	Press release Recommendations
New PCI-SSC guidance on phased-in implementation of Key Blocks	<p>The Payment Card Industry Security Standards Council published a blog post explaining the 3 phases of implementation of Key Blocks as required under the PCI PIN Standard. Key Blocks are used to protect the integrity of cryptographic keys. The objective of each stage of implementation of Key Blocks is as follows:</p> <ul style="list-style-type: none"> – Phase 1: implementation for internal connections and key storage; 	27 August 2019	PCI SSC blog post



Development	Summary	Date	Links
	<ul style="list-style-type: none"> Phase 2: implementation for external connections to associations and networks; and Phase 3: implementation to extend to all merchant hosts, point-of-sale devices and ATMs. <p>The phased-in implementation enables organisations to focus resources on the specific risks associated with each phase and to support smooth transition across the payments network.</p>		
Public consultation on use of big data analytics in insurance sector	<p>The International Association of Insurance Supervisors is using a public consultation to seek feedback on its draft Issues Paper on the use of big data analytics ("BDA") in insurance. BDA refers to the use of algorithms and advanced analytics by insurers to make decisions based on patterns and trends, and the availability of new alternative data sources. The public consultation closes on 16 October 2019.</p> <p>The paper examines how insurers are able to collect, process and use data throughout the various stages of the insurance product lifecycle, from product design to claims handling. It aims to enable understanding of the possible benefits and risks to customers related to the use of BDA by insurers.</p>	2 September 2019	IAIS consultation statement
EDPB thirteenth plenary session	<p>The EDPB convened for its thirteenth plenary session on 10-11 September 2019. The agenda comprised guidance on data subject rights, data portability and compensation to app users in exchange for their personal data, as well as a memorial tribute to Giovanni Buttarelli (the late European Data Protection Supervisor).</p>	10 September 2019	Agenda
Review of the implementation and enforcement of the EU-US Privacy Shield	<p>The International Trade Administration of the U.S. Department of Commerce ("DOC") produced a statement outlining the steps it has taken to implement and strengthen the EU-US Privacy Shield program. The measures include improving the certification process by using extensive company reviews, additional compliance monitoring, checks for false claims, active complaint resolution mechanisms and education initiatives to raise awareness of the program.</p> <p>As a result of the third annual review of the Privacy Shield program, the U.S. Federal Trade Commission ("FTC") revealed</p>	12 September 2019	DOC September statement DOC statement (12 September)



Development	Summary	Date	Links
	that they have taken seven new Privacy Shield-related enforcement actions to date since the previous review.		
Expert group established to consult on digital ethics in insurance	<p>The EIOPA has set up a consultative expert group on digital ethics in insurance to, among other things, facilitate the development of 'digital responsibility principles' in the sector. The move follows the association's review of the use of big data analytics in the motor and health insurance fields in 2018.</p> <p>The proposed principles will seek to address the use of new business models, technologies and data sources from the perspective of fairness taking account of ethical considerations, and will cover different areas of the insurance value chain – with a focus on pricing and underwriting, given their importance in the insurance sector.</p>	17 September 2019	EIOPA statement
Factsheet on ENISA and Cybersecurity Act	<p>The European Commission published an infographic factsheet about the European Agency for Network and Information Security ("ENISA") and the Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No.526/2013 ("Cybersecurity Act").</p> <p>The factsheet summarises the objectives of the Cybersecurity Act which are to scale up the EU's response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market.</p> <p>The factsheet also explains how the Cybersecurity Act will better enable ENISA to support EU Member States in dealing with cyber-attacks, by way of a strong mandate, a permanent status and adequate resources.</p>	11 September 2019	Press statement Factsheet
New Ad hoc Committee on AI established by Council of Europe	<p>The Committee of Ministers of the Council of Europe has created an Ad hoc Committee on Artificial Intelligence – an intergovernmental committee of experts to examine the feasibility of a legal framework for the development, design and application of artificial intelligence ("AI").</p> <p>The committee will consider the standards of the Council of Europe in the fields of human rights, democracy and the rule of</p>	12 September 2019	Committee statement



Development	Summary	Date	Links
	law and will carry out broad multi-stakeholder consultations to facilitate its work.		
New report on cyber risk for insurers	<p>The European Insurance and Occupational Pensions Authority ("EIOPA") published a report, "Cyber Risk for Insurers – Challenges and Opportunities". The report is based on responses from 41 large (re)insurance groups across 12 European countries (Austria, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Spain, Sweden and United Kingdom) and its aim is to further enhance the level of understanding of cyber risk for the European insurance sector.</p> <p>The report calls for the development of a cyber resilience framework, in particular, clear, comprehensive and common requirements on the governance of cybersecurity as part of operational resilience. The governance framework should include a set of definitions and terminology on cyber risks to enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector.</p> <p>The report refers to the recent growth of the cyber insurance market but underlines that non-affirmative cyber exposures (where cyber risk is neither explicitly included nor excluded within an insurance policy) remain a source of concern, which should be addressed.</p> <p>In addition, more data collection on cyber incidents and losses (such as a European-wide cyber incident-reporting database, based on a common taxonomy) would allow insurers to manage and price their affirmative cyber risk exposures more effectively.</p>	17 September 2019	EIOPA statement Report
ICC calls for WTO to prohibit tariffs on cross-border data flows	<p>The International Chamber of Commerce ("ICC") has published a paper 'The business case for a permanent prohibition on customs duties on electronic transmissions' which calls for World Trade Organization ("WTO") members to prohibit permanently the imposition of tariffs on cross-border data flows.</p> <p>A moratorium on customs duties on cross-border data flows has been in place since the WTO's Second Ministerial Conference in 1998. The report explores the economic disruption that would occur if the moratorium is lifted. The report also highlights that</p>	17 September 2019	ICC statement ICC paper



Development	Summary	Date	Links
	<p>any benefits to countries from tariff revenue on electronic transmissions are vastly outweighed by the disruptions to business and economic losses resulting from lifting the moratorium.</p> <p>The report comprises part of a series on various aspects of the WTO plurilateral Joint Statement Initiative on Electronic Commerce.</p>		
Latest draft of the proposed ePrivacy Regulation	<p>The Finnish Presidency of the Council of the EU has published various drafts of the proposed ePrivacy Regulation ("Regulation") in the context of a number of Working Party on Telecommunications and Information Society's meetings. The drafts are dated 12 July 2019, 26 July 2019, 18 September 2019 and 4 October 2019.</p> <p>By way of reminder, the Regulation will sit alongside the GDPR and is intended to repeal and replace the existing ePrivacy Directive 2002/58/EC (as amended) which governs – among other things – the confidentiality and security of communications services, the use of cookies and location data and the sending of direct marketing communications. It is broader in scope than the ePrivacy Directive and aims to cover communications provided by a wider range of providers, including over-the-top service providers (such as instant messaging apps), Voice over Internet Protocol platforms and machine-to-machine services (such as the Internet of Things).</p> <p>The current draft text provides:</p> <ul style="list-style-type: none"> – an extended scope to cover internet based electronic communication services (so-called "over the top" services) as well as traditional communications services; – a GDPR standard of consent applicable to activities covered; – new lawful grounds for processing communications data; – new rules on the uses of cookies, tracking technologies and the sending of unsolicited marketing communications; and – enhanced obligations around privacy by design and by default. 	4 October 2019	Draft text (12 July 2019) Draft text (26 July 2019) Draft text (18 September 2019) Draft text (4 October 2019)



Development	Summary	Date	Links
	<p>Failure to comply with the Regulation will have GDPR-style ramifications - including fines of up to 2% global annual turnover, or even 4% for certain breaches.</p> <p>Organisations should monitor progress of the draft Regulation and assess its relevance to any direct marketing activities and/or tracking technologies. Note that it is possible that the Regulation may not become law in the UK, if its date of application falls outside of any agreed transition period or if the UK leaves the EU without a deal before that date. However, the UK will be incentivised to adopt the Regulation, or comparable rules in order to, among other things, secure an adequacy decision from the EU in respect of data transfers.</p>		
European Parliament releases Guidelines on Ethics in AI	The European Parliament has released its 'Guidelines on Ethics in Artificial Intelligence (AI): Context and Implementation'. The guidelines aim to shed light on the ethical rules recommended when designing, developing, deploying, implementing or using AI products and services in the EU – including adhering to laws underpinning privacy and data protection, such as GDPR. The guidelines also identify the challenges with implementing such products and services, and outline ideas for future EU action ranging from soft law guidance to standardisation to legislation in the field of ethics and AI. The guidelines also give an overview of the main ethical frameworks for AI under development outside the EU (including in the United States and China).	19 September 2019	Guidelines
Europol and Financial Services Information Sharing and Analysis Center announce memorandum of understanding	The Financial Services Information Sharing and Analysis Center and Europol's European Cybercrime Centre announced they have signed a memorandum of understanding to tackle cybercrime across Europe, in an effort to facilitate the law enforcement response to cybercrime in the financial institutions sector through a 'symbiotic intelligence-sharing network'.	19 September 2019	Europol press statement
Application of the prohibition on processing sensitive personal data to search engine operators	In the case GC and Others v Commission nationale de l'informatique et des libertés (C-136/17) the CJEU ruled that operators of search engines are subject to the prohibition on processing sensitive data laid down in Article 8 of Directive 95/46/EC (and now in Article 9 of the GDPR).	24 September 2019	Press release CJEU judgment



Development	Summary	Date	Links
	<p>The CJEU had to answer several questions raised by the French supreme administrative court (Conseil d'Etat) following an appeal lodged by several people alleging that the La Commission Nationale de L'informatique ("CNIL") had wrongly refused to serve formal notice to Google, which had refused to de-reference links to third-party websites including sensitive data concerning them (eg relating to criminal proceedings, or revealing a religious opinion).</p> <p>In answer to the first question, the court considered that search engine operators have no responsibility for the processing of sensitive data on the referenced third party websites. However, they are data controllers for the processing involved in referencing the relevant webpages. The CJEU ruled that in so far as the activity of a search engine is liable to affect significantly (compared with that of website publishers) the fundamental rights relating to privacy and data protection, the operator of the search engine must ensure that, within the framework of its responsibilities, powers and capabilities, the activity meets the requirements of EU law.</p> <p>The CJEU held that in the context of de-referencing requests, a balance must be struck between the fundamental rights of the person requesting the de-referencing and those of internet users potentially interested in that information.</p> <p>The court also made clear that the restrictions relating to the processing of sensitive personal data and data related to criminal offences and convictions apply to all controllers carrying out such processing, including search engine operators. The search engine operator would be responsible, because of the referencing of third party web pages containing the relevant personal data in the list of results presented to internet users further to their search.</p> <p>A search engine operator may refuse to grant a request for de-referencing, in the case of data made public by the data subject, unless the data subject has the right to object to that processing on compelling legitimate grounds relating to his particular situation.</p> <p>The court emphasised that while, as a general rule, the data subject's rights override the freedom of information of internet users, this balance could change depending on the facts</p>		



Development	Summary	Date	Links
	<p>(including, the nature of the information, its sensitivity) and on the interest of the public in having that information. Search engine operators must use this information to ascertain whether the inclusion of a link in the list of results displayed following a search on the basis of the data subject's name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search.</p> <p>In addition – in relation to web pages containing data relating to criminal proceedings which no longer reflect the current situation – the search engine must assess whether someone has a right to the relevant information no longer being linked with their name by a list of results displayed following a search against their name by considering the circumstances (including the nature and seriousness of the offence, the progress and the outcome of the proceedings, the time elapsed, the part played by that person in public life and his or her past conduct, the public's interest at the time of the request, the content and form of the publication and the consequences of publication for that person). In cases where the individual's request is refused, the search engine is still required to adjust the search results list so that the message given to the internet user reflects the current legal position.</p> <p>The CNIL has announced that it will carry out an in-depth analysis of this decision in the coming days, and publish on its website a FAQ explaining its practical consequences.</p>		
New report on the role of AI and machine learning ("ML") in capital markets	<p>The Association for Financial Markets in Europe ("AFME") published a report on 'Artificial Intelligence and Machine Learning in Capital Markets: Considerations for a Broad Framework for Transparency'.</p> <p>The report proposes a technology-neutral, principles-based approach to transparency, built around the assumptions used in the development of AI/ML models and testing of those models, to meet stakeholder needs. The approach should be built around: (i) qualitative and quantitative assumptions; and (ii) testing. The frameworks should be tailored to the individual risk profile of the relevant AI/ML application and to the needs and knowledge of the various internal and external stakeholders. The framework should</p>	September 2019	Report



Development	Summary	Date	Links
	<p>also be evaluated and updated throughout the application's lifecycle.</p> <p>The report also recognises that the use of AI/ML must be consistent with obligations in key areas such as governance, accountability, duty to clients and data protection.</p>		
EU Blockchain Observatory and Forum publishes report on legal and regulatory framework of blockchains and smart contracts	<p>The European Union Blockchain Observatory & Forum published a thematic report which examines the intersection of blockchain and the law. The report comprises an overview of legal issues relating to blockchain technology and an examination of the legal implications of different kinds of smart contract.</p> <p>In terms of the interplay between blockchain and data protection, the report notes that there are three main areas of tension:</p> <ul style="list-style-type: none"> – the challenge of identifying controllers and processors, and enforcing their obligations; – the question over whether and how personal data can be truly anonymised; and – how data subjects can exercise their rights under GDPR in respect of personal data recorded on a blockchain. 	27 September 2019	Report



Austria

Contributors



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



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



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

Development	Summary	Date	Links
Austrian DPA publishes quarterly report	<p>In the Quarterly Report published by the Austrian Data Protection Authority ("DPA"), the DPA emphasised the formal requirements which need to be met for GDPR complaints. The amount of complaints has multiplied since GDPR came into force. According to the DPA, many of these complaints are unsuccessful.</p> <p>The DPA recommends that data subjects use the official complaint form on the DPA's website (www.dsb.gv.at).</p>	1 July 2019	<p>Quarterly Report by the Austrian DPA (in German)</p> <p>Website of the Austrian DPA (in English)</p>
Highest penalty under GDPR issued in Austria to date EUR 50,000	<p>The Austrian DPA recently imposed a fine of EUR 50,000 on an Austrian medical company. This is the highest fine issued under GDPR in Austria up to date.</p> <p>The company has appealed against the fine, therefore the fine is not final and the decision is not yet formally published.</p>	12 August 2019	Decision not yet published but case details can be found here .
Austrian DPA: data subject rights may not be made subject to special formal requirements	<p>An Austrian company included a clause in its data protection notice, declaring that the company would only answer Data Subject Rights Requests if they were sent directly to the company's Data Protection Officer ("DPO").</p> <p>A data subject sent a data access request in writing to one of the company's offices. The company ignored the request and the data subject filed complaint with the Austrian DPA.</p>	<p>Date of Decision: 2 February 2019</p> <p>Published: 16 July 2019</p>	Link to the decision by the DPA (in German)



Development	Summary	Date	Links
	The DPA ruled that according to Article 12 GDPR, it cannot be a requirement that data subjects must send data subject rights requests to a certain address or person. As long as the company was reasonably able to take notice of the request, it is obliged to answer the request within the timeframe of Article 12 GDPR.		
Austrian DPA: "Action cams" at rollercoasters or alpine coasters require valid consent or legitimate interest	<p>During many rollercoaster rides and similar attractions, it is common practice that, at the steepest point, a camera takes a picture of its customers, referred to as 'action cams'. After the ride, the customers can purchase a copy of these photos.</p> <p>An Austrian summer toboggan run operated an action cam. The toboggan run's operator included a clause in their Terms of Use according to which customers are assumed to have consented to this action cam taking his or her photo.</p> <p>The Austrian Data Protection Act includes specific rules for the processing of photo and video data (section 12 Austrian Data Protection Act).</p> <p>The Austrian DPA ruled that including such a consent clause in Terms of Use violates the prohibition of consent binding (Article 7 GDPR).</p> <p>The Austrian DPA ruled that including such a consent clause in Terms of Use violates the prohibition of consent binding (Article 7 GDPR).</p> <p>The operator of the toboggan run was therefore ordered to cease operating the action cam, unless it could either prove:</p> <ul style="list-style-type: none"> – that each data subject whose photo is taken has given their consent freely; or – that processing such video or photo data is based on the adequate legitimate interest of the operator. 	<p>Date of Decision: 2 February 2019</p> <p>Published: 7 August 2019</p>	Link to the decision by the DPA (in German)
Regional Court: Data subjects can claim EUR 800 in compensation for illegal processing of data on political opinion	<p>An Austrian newspaper found out that the Austrian Postal Services had combined the data available to them with data from public sources in order to create profiles of individual citizens. These profiles included data on the expected political affiliation of the individual.</p> <p>Some of these profiles were allegedly sold for marketing purposes.</p> <p>One individual, whose data was profiled in this way, filed a court claim for compensation against the Austrian Postal Services.</p>	16 August 2019	Newspaper article, including quotes from the non-published judgment (in German)



Development	Summary	Date	Links
	<p>The Regional Court Feldkirch ruled that the Austrian Postal Services must pay EUR 800 to the individual in compensation for the illegal processing of personal data.</p> <p>Both parties appealed against the judgement and the case is now to be decided by the Higher Regional Court Innsbruck.</p>		



France

Contributors



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



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



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

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

Development	Summary	Date	Links
La Commission nationale de l'informatique ("CNIL") guidelines on cookies and trackers	<p>Since the GDPR has strengthened the conditions for consent, the CNIL published new guidelines on cookies and trackers on 18 July 2019 to replace the existing recommendation on cookies and trackers of 5 December 2013. The new guidelines have been issued without waiting for the future ePrivacy regulation to come into force.</p> <p>The new guidelines apply to all operations involving cookies and trackers on any type of device, including smartphones, computers, and connected vehicles</p> <p>The CNIL clarifies that, pursuant to the GDPR and the EDPB guidelines on consent, the use of cookies and trackers is only possible once freely given, specific, informed and unambiguous consent has been obtained from users.</p> <p>Freely given consent: users must not suffer any major inconvenience if they refuse to give or withdraw their consent. It is not permitted to block access to a website or a mobile application, if the user does not consent to cookies, referred to as a 'cookie wall'.</p> <p>Specific consent: users must be able to specifically consent to each purpose of the processing. Blanket acceptance of</p>	4 July 2019	CNIL guidelines (in French)



Development	Summary	Date	Links
	<p>general terms and conditions of use does not constitute valid specific consent.</p> <p>Informed consent: information must be provided to users in clear and plain language. Users must be informed about the identity of the data controller(s), the purpose(s) of the cookies or trackers, and the existence of the right to withdraw consent to cookies at any time.</p> <p>Unambiguous consent: users must take a clear and positive action to give their consent to cookies. Merely continuing to browse a website or to use a mobile application after a cookie banner is displayed can no longer be considered valid consent. Similarly, the use of pre-checked boxes is not sufficient.</p> <p>Operators who use cookies and trackers will need to be able to prove that they have obtained explicit consent from the users.</p> <p>The guidelines will be supplemented with recommendations setting out practical methods for obtaining consent. These recommendations will be subject to public consultation before their final adoption by the CNIL which is expected in early 2020. Operators will have six months from the publication of the final recommendations to comply with the new rules on cookies and trackers.</p>		
CNIL grants its first accreditation for the certification of DPO skills	<p>On 4 July 2019, in accordance with the accreditation standard for the certification of DPOs adopted in September 2018, the CNIL granted its first accreditation to AFNOR CERTIFICATION, for a period of five years.</p> <p>As a reminder, on 20 September 2018, the CNIL adopted two standards for the certification of DPOs:</p> <ul style="list-style-type: none"> – a certification standard that sets out the conditions for the admissibility of applications and a list of 17 skills and know-how expected from a person applying to be certified as a DPO; – an accreditation standard that sets out the criteria applicable to organisations that wish to be authorised by the CNIL to certify DPOs on the basis of the certification standard. 	4 July 2019	CNIL publication (in French)



Development	Summary	Date	Links
	<p>The CNIL has reiterated that the certification is not mandatory to practise as a DPO, and it is not a requirement that a person is appointed as a DPO in order to apply for the certification.</p> <p>The CNIL also announced that its next certification project will focus on training in personal data protection.</p>		
Sanction of insurance company by the CNIL for breach of customer data security	<p>The CNIL imposed a penalty of EUR 180,000 on an insurance company, for failing to adequately protect the personal data of users of its website.</p> <p>Customers can request quotes, subscribe to contracts or access their personal profile through the company's website. In June 2018, the CNIL received a report from a client of the company, who indicated that he had been able to access the personal data of other customers through his account.</p> <p>An online investigation found that the company's customer accounts were accessible via hyperlinks, and that the personal data of customers (including copies of driver's licences, vehicle registration documents, and bank statements) was accessible by changing the numbers at the end of URL addresses.</p> <p>On the same day that the issue was reported, the CNIL alerted the company and asked it to remedy the breach. A few days later, the company informed the CNIL that measures had been taken to rectify the problem. However, when a new audit was carried out at the company's premises, it was revealed that the measures taken were not sufficient to prevent access to and protect the security of the company's customers' personal data.</p> <p>The CNIL decided on a fine of EUR 180,000 after taking into account the seriousness of the breach due to the sensitive nature of the data, and the number of people involved, but also the company's cooperation with the CNIL and its reactivity in attempting to remedy the problem.</p>	25 July 2019	CNIL publication (in French)
The CNIL publishes a new template of record of processing activities	To support organisations' GDPR compliance efforts, the CNIL has published a simplified template to record data processing activities, in spreadsheet format.	25 July 2019	CNIL publication (in French)



Development	Summary	Date	Links
	<p>It contains a tutorial sheet to help professionals design and maintain the record, a sheet to list the data processing activities, and a sample sheet to fill in with the details of each processing activity.</p> <p>The CNIL's objective is that this template can be used for any type of processing, in order to help the professionals to meet their obligation under Article 30 of the GDPR.</p>		
Decisions relating to the right of opposition and Google My Business	<p>At the request of two individual healthcare professionals, two courts of first instance have issued interim orders to delete the claimants' listings on Google My Business ("GMB") due to negative reviews.</p> <p>The first interim order was issued by the Civil Court of Metz (TGI de Metz). A psychiatrist noticed negative reviews from alleged patients on his GMB listing. Google asserted it was not at fault for establishing the listing because it had used publicly-available data from professional directories and Google did not require the professional's consent, because it had a legitimate interest in providing such information to consumers.</p> <p>The court decided that total deletion of the listing would violate the principle of freedom of expression and for this reason, it also refused to lift the anonymity of the clients who had left reviews. The court concluded that it was not 'justified to force the deletion of negative comments by means prejudicial to privacy in order to preserve a practitioner's reputation'.</p> <p>In the second interim order of the Civil Court of Paris (TGI de Paris), Google Ireland was ordered to provide a dentist with the identification details of an internet user who posted an opinion on the dentist's GMB listing which could have caused him harm.</p> <p>The court held that one of the disputed comments was offensive, and that the dentist had a legitimate ground to request the identification details of the internet user to be able to initiate a compensation procedure.</p>	11 and 16 July 2019	<p>Decision of the court of Metz (in French)</p> <p>Decision of the court of Paris (in French)</p>



Development	Summary	Date	Links
	However, as in the case of the Civil Court of Metz (mentioned above), the Parisian judge dismissed the professional's request to delete his listing because there was no legitimate reason.		
Decision on the unlawful collection of data and their use in litigation	<p>By an interim order issued on 2 August 2019, the Civil Court of Paris dismissed a Canadian film production company's request to obtain disclosure from an internet service provider ("ISP") of identification data concerning IP addresses linked to alleged illegal downloads.</p> <p>The Canadian company had noticed the presence of its works on online file-sharing platforms offered for downloading without its authorisation. It commissioned a German company to collect traffic data in connection with these allegedly illegal downloads, and a list of 895 IP addresses relating to these acts was compiled between November 2017 and December 2018.</p> <p>In the first interim order, the Civil Court of Paris ordered the ISP to collect the identification data of the persons linked with these IP addresses, in order to provide it to the Canadian film production company.</p> <p>However, the ISP raised the question of the lawfulness of the data collection and processing of these IP addresses and the court approved its arguments.</p> <p>The court held that the collection of such data was a profiling operation with the purpose of monitoring the behaviour of individuals in the EU. As a result, the Canadian company, as a data controller established outside the EU, should have:</p> <ul style="list-style-type: none"> – appointed a European representative; – kept a record of processing activities in which this list of IP addresses should have appeared; – appointed a DPO because it was collecting data relating to criminal offences on a large scale; and – put appropriate safeguards in place for the transfer of the data to a country outside the EU. <p>The Parisian court concluded that the processing of such IP addresses constituted an unlawful and disproportionate</p>	2 August 2019	Decision of the court of Paris (in French)



Development	Summary	Date	Links
	infringement of the relevant individuals' fundamental right to protection of their personal data.		
CNIL guidelines on the recording of videos, telephone conversations, and screenshots at work	<p>Certain devices which record telephone conversations can simultaneously screenshot the image that appears on an employee's computer screen or can video record the screen activity during the call. The CNIL considers these devices to be particularly intrusive and so they must be strictly controlled, because they may enable access to or monitoring of employees' private information (including personal emails, instant messaging conversations or confidential passwords). The CNIL considers that screenshots are disproportionate and irrelevant because they capture a fixed image of an isolated action, which cannot accurately represent the whole of an employee's activity. Therefore, employers are advised not to take such screenshots.</p> <p>The CNIL regards the video recordings of the screen to be a more accurate reflection of an employee's action because they can continuously monitor the screen activity. Consequently, the use of video recording of screens coupled with telephone conversations can only be used by employer's in certain circumstances.</p> <p>The use of video recordings must be for the sole purpose of training staff and must be subject to the effective implementation of the following guarantees:</p> <ul style="list-style-type: none"> – employees are informed that they are being recorded; – the video recording is limited to the window of the business application to which the training relates; – the device is only active during a telephone call; – the use of such recordings should only concern people who have a genuine need for training on a business application or software programme; – the number of recordings must be proportionate to the need for training and strictly limited to the amount necessary to analyse these recordings for training purposes; 	17 September 2019	CNIL guidelines (In French)



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – video recordings of others must be anonymized; and – access to records is limited to authorised persons only. <p>The CNIL guidelines also emphasise that, given the potential impacts and risks of misappropriation of data and surveillance associated with these devices, the coupling of telephone recordings with any image (still or moving) of the employee's actions is disproportionate when used for purposes other than training, such as staff appraisal or internal fraud prevention.</p>		



Germany

Contributors



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



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



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



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



Sara Ghoroghy
Associate
T: +49 40 808094 446
saraghoroghy@
eversheds-sutherland.com

Leopold Beer
Trainee

leopoldbeer@
eversheds-sutherland.com

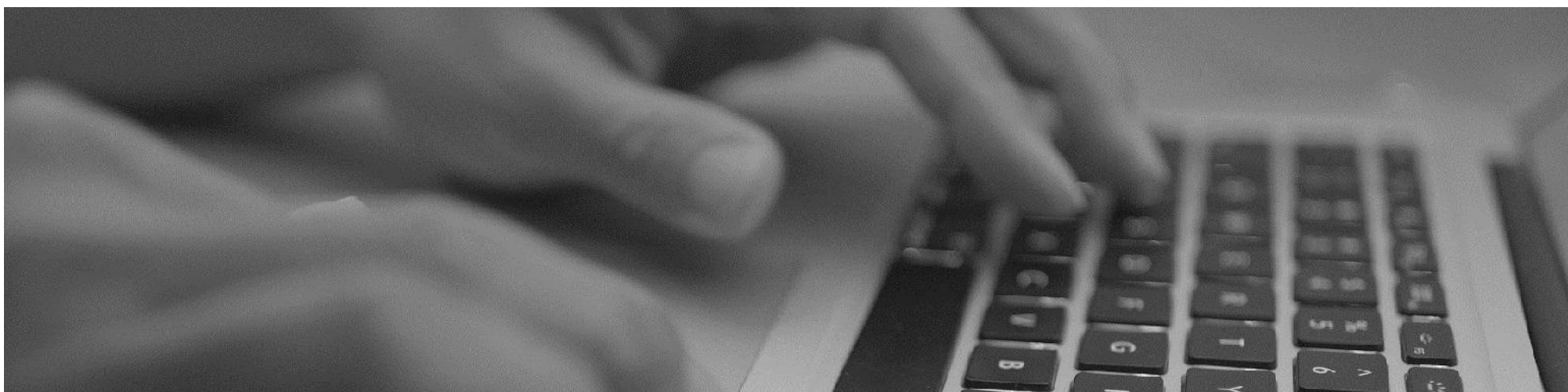
Development	Summary	Date	Links
The right of access referred to in Article 15 GDPR is comprehensive	<p>The Higher Regional Court Cologne ("HRCC") determined in its judgement that the GDPR grants a comprehensive right of access and the term "personal data" is to be interpreted widely.</p> <p>According to the HRCC, statements that provide a subjective and/or objective assessment of an identified or identifiable person also have a personal element thereby falling under the definition of "personal data". The defendant argued that it was economically impossible for large companies to search and secure the large volumes of files containing personal data, however the HRCC rejected this contention and asserted that all enterprises concerned with processing electronic data have the responsibility to do so in accordance with data protection legislation.</p>	26 July 2019	Judgment
Attorneys need a Power of Attorney ("POA") in order to exercise the right of access for clients	A district court of Berlin decided that a lawyer must be granted a POA in order to exercise the right of access under Article 15 GDPR. This is necessary in order to ensure that personal data does not fall into the wrong hands. The necessity also derives from Article 12(6) GDPR, according to	29 July 2019	Judgment not published at time of publication



Development	Summary	Date	Links
	which the data controller must request additional information, if necessary for the confirmation of the identity of the person requesting access to personal data. This is of even greater importance when a subject access request to personal data is submitted on behalf of someone else.		
A chairperson of a German Workers' Council can be a DPO of a corporation without a conflict of interest	The Saxon State Labour Court ruled that the chairperson of a German Workers' Council (an organisation which represents employees) can also be the company's DPO and that there is no conflict of interest between these activities.	19 August 2019	Judgment
Bavarian Data Protection supervisory authority published an FAQ on numerous GDPR questions	The Bavarian Data Protection supervisory authority ("BDPSA") has published a comprehensive FAQ answering over 100 questions in relation to various GDPR. It is important to note that the BDPSA's assessment is not binding for the courts. The FAQ outline the BDPSA's opinion on issues such as the use of Google Analytics on websites without the consent of the user, the integration of social plugins, the use of dashcams in cars and the requirement for a data breach to be reported within a 72 hour period.	1 September 2019	FAQ
The storage of generally accessible personal data for "cold calls" is inadmissible	A company stored the contact information of various other companies in order to call them without prior consent. The contact details were publicly available. The competent data protection supervisory authority considered this to be a breach of data protection law and issued a notice to that effect. The Higher Administrative Court of Saarland confirmed that even if contact information is publicly available, it may not be stored for marketing purposes if the data subject to whom the contact details refer, has not given consent or if there has not been a previous business relation between the parties.	10 September 2019	Judgment
The data protection supervisory authority may prohibit the operation of a Facebook fan page	<p>According to the ruling of the Federal Administrative Court, a data protection supervisory authority ("DPSA") can order an operator of a Facebook fan page to deactivate the fan page if the digital infrastructure provided by Facebook has serious data protection deficiencies. The decision follows the order issued by the DPSA of Schleswig-Holstein, which required an educational institution based in Kiel to deactivate such a fan page.</p> <p>The decision acknowledges that Facebook can access the personal data of internet users who visit fan pages without informing them of the type, scope and purpose of the data collection in accordance with the provisions of the German Telemedia Act and of their right to object to the creation of a user profile for advertising and market research purposes.</p>	11 September 2019	Press statement



Development	Summary	Date	Links
New GDPR fines imposed against Delivery Hero and N26	<p>In August 2019, the Berlin Data Protection Commissioner (“BDPC”) imposed fines in the total amount of EUR 195,407 against Delivery Hero Germany GmbH. The decision is legally binding, and the fines were imposed by the BDPC for various individual breaches of data protection law by the company. The majority of the incidents concerned the non-compliance with the protection and security of data subject rights. According to the findings of the BDPC, Delivery Hero had not deleted accounts of former customers in ten cases, even though those accounts had been inactive on the company’s delivery service platform for several years.</p> <p>The company N26 had blacklisted the names of former customers for money laundering prevention purposes, regardless of whether they were actually suspected of money laundering. N26 has also accepted the fine and announced a number of measures to the BDPC to remedy previous organisational shortcomings.</p>	19 September 2019	Press statement
New guidance for financial services organisations on outsourcing to cloud service providers	Germany’s Federal Financial Supervisory Authority has issued guidance on outsourcing to cloud service providers. The guidance is aimed at financial institutions, insurance providers, pension funds, investment services enterprises, capital management companies and payment and e-money service providers.	20 September 2019	Guidance



Hungary

Contributors



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

Ádám Takács
Paralegal

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



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

Development	Summary	Date	Links
Resolution of the National Authority for Data Protection and Freedom of Information ("NADP") regarding the operation of security cameras	<p>The NADP issued guidance in a case regarding data processing with a camera operated by a natural person. The cameras were used for property and personal security purposes, and recorded both private property but also public areas.</p> <p>If the data processing of personal data had been by a natural person in the course of a purely personal or household activity, it would fall outside the material scope of the GDPR. However, the cameras in question operated with an inadequate masking function, meaning that they monitored both public and other private areas.</p> <p>As there was no legal basis for the processing of this data, the operation of the cameras breached the provisions of the GDPR.</p>	<p>Decision: 26 June 2019 Published: 1 July 2019</p>	<p>NADP resolution (Hungarian language only)</p>
The NADP issues guidance for data processors	<p>The NADP published guidance on the requirements which data processors should meet to ensure there is a balance of interests and to support any assertion that they have a legitimate interest in the relevant data processing activities.</p> <p>The guidance was published following a case in which the applicant petitioned for the data processor to delete all his phone and e-mail contact data and to only contact the applicant via post. The data processor refused this claiming that these contact methods served the legitimate interest of the business, which only retains the data based on a balance of interests test.</p> <p>The NADP held that because the applicant is able to receive correspondence by post, the other contact data is unnecessary and should be deleted. The</p>	<p>Decision: 26 June 2019 Published: 1 July 2019</p>	<p>NADP resolution (Hungarian language only)</p>



Development	Summary	Date	Links
	NADP found that the company had not been able to substantiate its argument that it had a legitimate interest in keeping the phone and e-mail contact data, which it would not need to use.		
The NADP dismisses an application for the removal of news article from the internet	<p>The applicant in the case requested the removal of an article from the internet because he believed it contained incorrect data, misrepresented him and adversely affected his reputation.</p> <p>The NADP dismissed the application referring to Article 85 of the GDPR and the Hungarian data protection and freedom of press laws, which both state that the further retention of the personal data should be lawful where it is necessary for exercising the right of freedom of expression and information, including processing of data for journalistic purposes or the purposes of literary or artistic expression.</p>	31 July 2019	NADP resolution (Hungarian language only)
The NADP issues statement on investigation into voice recording by Facebook	<p>Facebook asserts it has stopped the practice of listening and analysing recorded conversations, but the NADP is waiting for a written guarantee. The NADP appreciates that Facebook has decided to suspend the analysis of the recorded audio material, nevertheless it will participate in the EU-wide investigation into the data management of Facebook.</p> <p>In its statement, the NADP highlighted the social responsibility of technology companies, which involves the protection of freedom of expression in both the public and private sphere, and the need for censorship-free social networking sites.</p>	14 August 2019	NADP statement (Hungarian language only)

Ireland

Contributors



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



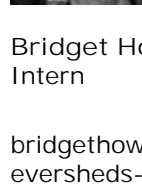
Neasa Ní Ghráda
Senior Associate
T: +35 31 66 44 25 8
neasanighrada@
eversheds-sutherland.ie



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



Stephanie White
Trainee
T: +35 31 66 44 92 0
stephaniewhite@
eversheds-sutherland.ie



Bridget Howard
Intern
bridgethoward@
eversheds-sutherland.ie

Development	Summary	Date	Links
A transparent process: Data Protection Commissioner ("DPC") guidance on data sharing in the public sector	Eversheds Sutherland analyses the guidance published by the DPC on data sharing in the public sector (published in May). The DPC noted its support for developing more efficient and customer-centric public services and sought to clarify the public sector obligations relating to processing personal data in the delivery of public services in a way which is lawful, fair and transparent.	July	Eversheds Sutherland briefing
Irish DPC issues guidance on CCTV for controllers	Eversheds Sutherland analyses the guidance published by the DPC on CCTV usage for data controllers. The guidance is intended to assist owners and occupiers of premises to understand their responsibilities and obligations regarding data protection when using CCTV. This is particularly relevant for premises that are workplaces or are otherwise accessible to the public.	July	Eversheds Sutherland briefing DPC article
DPC publishes the fourth episode of its official podcast 'Know Your Data'	In episode four, the Head of Communications of the DPC, Graham Doyle, answers common questions which the DPC receive relating to CCTV in the home.	9 July 2019	DPC press release Podcast can be found here
DPC publishes a preliminary report on Stream II of the DPC consultation on processing children's personal data and the rights of children as data subjects	The DPC has completed Stream II of the public consultation on the data rights of children under the GDPR. Stream I engaged adult stakeholders whereas Stream II engages children and young people. The preliminary report highlights the level of engagement received by the DPC and the general feedback of young people in relation to data protection. This feedback will be taken into consideration by the DPC while drafting their guidelines on the matter.	29 July 2019	DPC press release



Development	Summary	Date	Links
DPC issues guidance on data collected by apps	The DPC has issued advice on the use of personal data by apps to provide a service. The guidance outlines that the privacy policies of apps should explain why the collection of personal data is necessary for the apps functionality. The guidance provides steps which data subjects should take before signing up to apps in order to protect their personal data.	31 July 2019	DPC guidance
Welcome data breach guidance issued by the DPC	Eversheds Sutherland published an article analysing the guidance published by the DPC on GDPR breach notifications. 'The Guidance will prove an effective tool for all controllers and processors when faced with a data breach scenario in recognising the steps to be taken to comply with data protection law.'	August	Eversheds Sutherland briefing
DPC publishes the fifth episode of its official podcast 'Know Your Data'	In episode five, the Head of Communications of the DPC, Graham Doyle, answers questions relating to taking photos at school events.	9 August 2019	DPC press release
DPC publishes guidelines on data breaches for controllers	The Guidance outlines what constitutes a data breach and the obligations for data controllers under the GDPR following such an event.	12 August 2019	DPC guidance
DPC publishes the report of its investigation into the Public Services Card issued by the Department of Social Protection and the Department of Public Expenditure	<p>In August, the DPC published a highly critical report in which it stated that the Government had no legal basis for requiring the public get a Public Services Card to access public services such as welfare payments and passport renewals. The DPC further required that the Government delete the personal data held by Governmental Departments, claiming that the retention of such information contravenes Data Protection Law.</p> <p>There has been push back from the Government on this issue, and various Departments have released statements citing the legal advice they have received from the office of the Attorney General stating they do have a legal basis for the processing of this data.</p> <p>It is likely that this issue between the two public bodies could end up in court, as the Departments are unlikely to comply with any enforcement notice issued by the DPC.</p>	<p>DPC's statement was published on 16 August 2019</p> <p>The Report was published on 17 September 2019</p>	DPC's statement
DPC publishes guidelines on documents required to raise a concern with the DPC	The DPC issued guidelines on the required documentation necessary to be included for in data protection query to the DPC.	29 August 2019	DPC guidelines



Development	Summary	Date	Links
DPC publishes guidelines on what to do if private data is found in a public place	The DPC has published guidance for incidents where personal data in hard copy form are found by a member of the public. The DPC advises members of the public to, if possible, immediately return the document to the data controller. When the controller cannot be identified the individual should contact the DPC for assistance in returning the document to the rightful owner.	5 September 2019	DPC guidelines
DPC publishes highlights from Stream I of the public consultation on children's data protection rights	The DPC published the submissions from Stream I of the public consultation on children's data protection rights. Stream I engaged adult stakeholders whereas Stream II engaged children and young people.	9 September 2019	DPC press release
DPC publishes the sixth episode of its official podcast 'Know Your Data'	In episode six, the Head of Communications of the DPC, Graham Doyle, addresses what Brexit will mean for organisations who transfer personal data from Ireland to the UK.	16 September 2019	DPC press release
DPC issues guidance on direct marketing	The DPC issued guidance for data subjects on direct marketing. The guidelines outline what direct marketing is, what constitutes unsolicited direct marketing and how individuals can opt out of direct marketing.	18 September 2019	DPC guidelines

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



Sebastian Vanegas
Trainee
T: +39 06 89 32 70 56
sebastianvanegas@
eversheds-sutherland.it



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

Development	Summary	Date	Links
Italian Data Protection Authority ("IDPA"), jointly with the Italian Competition Authority and the Italian Telecommunication Authority (jointly the "Authorities"), publish guidelines on Big Data	The Authorities issued the 'Guidelines and policy recommendations on Big Data' as a result of a dedicated inquiry. The inquiry sought to better understand the implications of the development of the digital economy based on the analysis of increasingly large volumes of data, for privacy, regulation, anti-trust and consumer protection.	IDPA's press release published: 10 July 2019	IDPA's English press release Authorities' inquiry on Big Data- Guidelines and policy recommendations (only available in Italian)
IDPA rules on processing of special categories of personal data	IDPA's published its prescriptions (rules) on the processing of special categories of personal data, pursuant to article 21 of Legislative Decree 101/2018 (amending the Italian Privacy Code). The publication came at the end of the revision procedure of the 'General Authorizations'. The 'General Authorizations' were issued under pre-GDPR Italian data protection law to regulate the processing of special categories of personal data in specific contexts. The IDPA prescriptions collate the 'General Authorizations' that are still applicable after the entry into force of the GDPR. The prescriptions contain the obligations to be complied when processing special categories of data in the context of: – employment;	Prescriptions published: 29 July 2019 in the Official Italian Journal	IDPA measure (only available in Italian)



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – associations, foundations, churches and religious associations and communities; – private investigations; – processing of genetic data; and – processing for purposes of scientific research. 		
Data Protection Officer's Handbook	IDPA helped develop a new DPO Handbook, dedicated to the DPOs of public entities, available on its website. The handbook was issued as part of the international project 'Training for Data' ("T4DATA") in which IDPA took part. T4DATA provides various training activities, organized by IDPA in coordination with other Data Protection Authorities.	Press release published: 5 August 2019	DPO handbook (English)
Notification of data breaches to IDPA	<p>IDPA issued a measure on the notification of data breaches, including a model form to be used for such purpose.</p> <p>This measure and model form repealed and replaced certain pre-GDPR forms of notification to IDPA (eg breaches in biometrics and in the circulation of information in the banking sector).</p>	<p>Measure dated: 30 July 2019</p> <p>Measure made available: 6 September 2019</p>	IDPA measure (only available in Italian)
Code of conduct pursuant to article 40 GDPR	<p>IDPA approved a code of conduct for 'credit information systems' managed by private entities. Among its provisions, this code of conduct:</p> <ul style="list-style-type: none"> – specifies categories of data relevant for the processing activities considered by the code of conduct; – provides for legal bases (legitimate interests) for the relevant data processing, security measures and retention periods; and – includes forms of information notices to be provided to relevant data subjects. <p>IDPA underlines that in any case the effectiveness of the code of conduct is made conditional on the completion of the accreditation phase of the monitoring body provided by the code of conduct before the EDPB, as under article 41 GDPR.</p>	<p>Measure dated: 12 September 2019</p> <p>Measure made available: 19 September 2019</p>	IDPA measure (only available in Italian)
IDPA Newsletter N. 457 of 23 September 2019	<p>IDPA published its periodic newsletter, which includes news of the following:</p> <ul style="list-style-type: none"> – commencement of the '2019 Privacy Sweep', an international inquiry dedicated to the management of data breaches. This initiative is 	<p>Published: 23 September 2019</p>	IDPA newsletter



Development	Summary	Date	Links
	<p>coordinated by the Global Privacy Enforcement Network (“GPEN”). IDPA takes part in this sweep and announced that it will focus its assessments on e-commerce activities;</p> <ul style="list-style-type: none"> – IDPA explained that companies providing diagnostic devices cannot use patients’ data for their own purposes. Local health authorities can communicate healthcare data to third parties only if there is an appropriate legal basis. An IDPA investigation revealed a local health authority, (before the entry into force of the GDPR) making patients’ healthcare data obtained through medical devices available to a third party company. The company anonymized and pseudonymized data in order to annex images to the documents filed to participate to a public tender (and later to a litigation). IDPA deemed that the communication of patients’ data from the local health authority to the company was unlawful, as it had no appropriate legal basis. The processing activities performed by the company on the patients’ data were also deemed unlawful as the company performed these processing activities for purposes other than those for which the company was designated as data processor by the local health authority (eg maintenance activities). IDPA has commenced sanction proceedings accordingly. 		

Latvia

Contributors



Elina Mucina
Partner

T: +371 67 280 102
elina.mucina@
eversheds-sutherland.lv

Development	Summary	Date	Links
First significant fine imposed in Latvia	<p>On 26 August 2019 the director of the Latvian Data State Inspectorate ("DSI") imposed a EUR 7,000 fine on a merchant providing services to an online store for failure to observe data subject's rights and failure to cooperate with the DSI. The merchant failed to reply in due time to the data subject regarding his request to erase personal data and subsequently failed to cooperate with the DSI by not providing the necessary information in a timely manner and not complying with the order issued by the DSI under article 58(2)(c) and (g) of the GDPR and article 23 of the Latvian Personal Data Processing Law.</p> <p>In 2018 the data subject had repeatedly contacted the merchant requesting the erasure of all personal data that the merchant had obtained as part of the data subject's order with the merchant, including mobile phone number. After requests to erase personal data, the merchant sent commercial messages via text message to the data subject's mobile phone.</p> <p>This is the first significant fine imposed by the inspectorate after the effective date of GDPR. The fine demonstrates to companies that even a complaint from a single individual may result in a substantial fine. As the DSI has confirmed on several occasions, it is in the interests of any controller to cooperate with the DSI and provide timely responses to its requests.</p>	Published: 29 August 2019	DSI statement (in Latvian) EDPB statement (in English)



Contributors

Lithuania



Rintis Puisys
Partner
T: +370 5 239 2373
rintis.puisys@
eversheds.lt

Linas Mockevicius
Associate
T: +370 5 239 2391
linas.mockevicius@
eversheds.lt

Development	Summary	Date	Links
The State Data Protection Inspectorate has published its semi-annual activity report	<p>The State Data Protection Inspectorate ("SDPI") published its report regarding its activities in the first six months of 2019 (hereinafter – the "Report"). The Report provides statistical data on various types of activities that were performed by the Inspectorate.</p> <p>The Report indicates that the SDPI has provided 2,332 consultations, 1.492 of which were addressed to data controllers and/or processors with the remainder provided to data subjects.</p> <p>Within the first six months of 2019, SDPI received 431 complaints. 495 complaints (including those received in 2018) have been investigated.</p> <p>There were a total of 110 directions imposed by the SDPI. Most of the directions (72) were instructions, 43 of them were reprimands. Additionally there was one EUR 61,500 fine imposed by the SDPI.</p> <p>The Report states that most of the directions (42) were imposed on providers of goods and services, 17 were applied to state and municipality enterprises while there were 13 sanctions applied to natural persons.</p> <p>As for the investigations, SDPI is said to have performed 26 investigations into data controllers' activities. There were 7 investigations that showed no breaches. In cases where breaches had been discovered, SDPI imposed one fine, 16 instructions and four recommendations.</p>	Published: 12 July 2019	SDPI press release (in Lithuanian)
SDPI has published the Guidelines on Personal Data Safety Measures and Risk Evaluation for public consultation	<p>The SPDI has published Guidelines on Personal Data Safety Measures and Risk Evaluation.</p> <p>The guidelines are being issued in respect of the GDPR requirement to ensure appropriate technical and organizational measures are in place in order to ensure a level of security of personal data.</p>	Published: 9 August 2019 Consultation closes: 30 September 2019	Guidelines (in Lithuanian)



Development	Summary	Date	Links
	<p>The guidelines are drafted by taking into consideration the European Union Agency for Cybersecurity recommendations 'Handbook on Security of Personal Data Processing' as well as ISO standards ISO/IEC 27001:2017 and ISO/IEC 27002:2017 and are intended to assist small and medium-size enterprises (SMEs) in their compliance with GDPR.</p> <p>The guidelines prescribe the specific technical and organizational measures that should be implemented by data controllers and processors, taking into account the level of risk. The level of risk is to be established by each controller/processor in line with the procedure prescribed in the Guidelines. The guidelines prescribe for three levels of risk (low, medium and high), each of which require that the specified technical and organizational measures are put in place by data controllers/processors.</p> <p>The guidelines were subject to public consultation which closed on 30 September 2019 and are expected to be adopted by year-end.</p>		
SDPI investigates hotels' implementation of data minimisation principle	<p>The SDPI has published a summary of its investigation of hotels' implementation of the data minimisation principle in the context of processing guest personal data.</p> <p>In respect of the scope of personal data processed, it was found that 16 out of 18 audited hotels implement the data minimisation principle. It was established that 2 hotels are processing the data on the place of birth of the guests. Whilst the hotels did not provide arguments for the necessity of processing such data, in SDPI's view, such processing is in breach of the data minimisation principle.</p> <p>It was also established that 4 hotels do not maintain records of processing activities in breach of Article 30 GDPR. The SDPI noted that it was obvious that the processing of guests' personal data by the hotels is not occasional, therefore, hotels do not fall under the exemption established in the Para 5 of Article 30 GDPR.</p> <p>SDPI has ordered the hotels to address the detected breaches. No sanctions have been imposed as a result of the breaches identified.</p>	Published: 26 September 2019	SDPI Press release (in Lithuanian)

Netherlands

Contributors



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



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



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

Development	Summary	Date	Links
Banks are not allowed to use transactional data for direct marketing purposes	The Dutch Data Protection Authority (Dutch: Autoriteit Persoonsgegevens) ("Dutch DPA"), has stated that banks are not allowed to use transactional data for direct marketing purposes. Direct marketing means – in this context - personalised advertising based on payment data of individual customers. Banks in the Netherlands were planning to use personal data of their customers for direct marketing purposes. However, due to (the amount of) complaints received by the Dutch DPA, they decided to interfere. The Dutch DPA sent a letter to the Dutch Banking Association (Dutch: Nederlandse Vereniging van Banken). This letter contains the aspects that must be taken into account when assessing whether the use of transactional data for direct marketing purposes can be considered compatible with the purposes for which the personal data was initially collected by the banks.	Published: 3 July 2019	DPA newsletter (in Dutch)
Hospital receives an administrative fine due to insufficient security measures. Breach of article 32 GDPR	The Dutch DPA has imposed an administrative fine of EUR 460,000 on the Haga Hospital in The Hague (Dutch: Stichting HagaZiekenhuis), because the hospital has not met and does not meet the requirements of two-factor authentication for the access to medical records and the regular assessment of log files in the period from October 2018. Besides an administrative fine, a penalty for non-compliance has been imposed due to the ongoing violation of GDPR. Reason of investigation	Published: 16 July 2019	Decision (in Dutch) Report (in Dutch)



Development	Summary	Date	Links
	On 4 April 2018, the hospital reported a data breach to the Dutch DPA. This data breach was related to unlawful access to patient records of a well-known Dutch national. In the report, the hospital announces that it will take security measures in anticipation of the internal investigation into unauthorised access to this patient file. The Dutch DPA stated that as the hospital has taken insufficiently appropriate measures with regard to the security aspects 'authentication' and 'control of the logging', the hospital has thereby breached article 32 GDPR.		
Dutch trade association for IT, telecom and internet companies launches GDPR-certification program within the meaning of article 40 GDPR	<p>The Dutch trade association for IT, telecom and internet companies in the Netherlands (Dutch: Nederland ICT), has launched a GDPR-certification program for Dutch organizations that process or wish to process personal data. After passing the certification audit, the relevant organization would receive a 'Data Pro-Certificate'.</p> <p>The underlying Code of Conduct – within the meaning of article 40 GDPR - that has been drawn up, has been submitted for approval to the Dutch DPA. A draft decision has been published in which the Dutch DPA indicate their intention to approve the Data Pro Code.</p> <p>The Data Pro-Certificate is valid for one year from the time of issue. The Data Pro-Certificate enables organizations to show they are compliant with the Data Pro Code and the GDPR.</p>	Published: 13 August 2019	DPA newsletter (in Dutch)
Dutch DPA finds that Microsoft has improved its privacy protection, but further investigation is required	<p>In 2017, the Dutch DPA found that Microsoft was using telemetry to unlawfully process users' personal data. In April 2018 Microsoft made several changes to Windows at the insistence by the Dutch DPA.</p> <p>The Dutch DPA has concluded that Microsoft has improved its privacy protection, but the Dutch DPA has stated that further investigations are required. The Dutch DPA also discovered new potentially unlawful instances of personal data processing. It has therefore asked the Irish Data Protection Authority to carry out a further examinations regarding the privacy of Windows-users.</p>	Published: 27 August 2019	DPA newsletter (in Dutch) Press release
Court ruling on article 82 GDPR	<p>On 2 September 2019, the Dutch District Court of Amsterdam has awarded a claimant financial compensation based on article 82 GDPR for non-material damages due to the sharing of the claimant's sensitive personal data without a legal basis.</p> <p>When working for her former employer, the claimant became partially incapacitated for work as a result of the burn-out she suffered at that time.</p>	Published: 2 September 2019	Court's decision (in Dutch)



Development	Summary	Date	Links
	<p>During her recovery, the employee started working for a new employer. The Dutch Employee Insurance Agency (Dutch: Uitvoeringsinstituut Werknemersverzekeringen) wished to send a letter to the former employer of the claimant regarding illness benefits that the claimant was entitled to. However, the Dutch Employee Insurance Agency accidentally sent the letter to her new employer instead of her former employer. The new employer of the claimant was not familiar with the partial incapacity of the claimant.</p> <p>The Dutch District Court of Amsterdam concluded that due to the sharing of claimant's personal data without a legal basis, the GDPR has been infringed and the claimant had suffered non-material damage.</p> <p>The information regarding the partial incapacity of the claimant must be qualified as sensitive personal information, and sharing this personal data with a third party may lead to serious negative consequences for the employee. The Dutch District Court of Amsterdam also determined that the Dutch Employee Insurance Agency should have investigated the consequences before sending the letter, instead of relying on an automated system. Due to the loss of control over her personal data and the fear and stress caused by the infringement, the Dutch District Court of Amsterdam ruled that the Dutch Employee Insurance Agency is obliged to pay the claimant EUR 250.</p>		
Court ruling on article 15 GDPR	<p>The case was initiated by a claimant who filed a request at a local church to disclose all personal information that they were processing about her. The claimant was convinced that within the church organization she was the subject of defamation and slander.</p> <p>The church answered the claimant in general terms. Dissatisfied about the church's answer, the claimant brought her request to the Court of First Instance as she was of the opinion that the disclosed personal information was insufficient. In the first instance the church argued that this was all a fishing expedition and also that offering her more information would involve confidential information of other church members, their personal opinions as well as internal memos of the church counsel. The church successfully argued that this information was not subject to the obligation of disclosure/right to access.</p> <p>This decision was appealed and heard by the Dutch Court of Appeal in The Hague. According to the Dutch Court of Appeal in The Hague, the GDPR does not contain an explicit exception on the right to access for internal or confidential information/memos. Thus, in this case all information stored in</p>	<p>Published: 17 September 2019</p>	<p>Court's decision (in Dutch)</p>



Development	Summary	Date	Links
	<p>the churches systems fell within the scope of the GDPR (article 2(1) GDPR). Thus, the claimant had a principal right of access.</p> <p>The above means, contrary to the ruling of the Court in First Instance, that the right of access is not blocked or restricted because the relevant documents could contain confidential information, internal correspondence, or could include personal thoughts and/or advice drafted for internal meetings and/or decision making.</p> <p>Although the Dutch Court of Appeal in The Hague understood that the church did not want to grant access to confidential information, the church was not allowed to block the right of access on the basis of confidentiality. A church also needs to respect the fundamental rights of the claimant of the protection of her personal life. The church is only allowed to limit the right to access confidential documents if this is necessary for the protection of the rights and freedom of others, in this case the personal rights of the church council members. The personal opinions of the members of the church council fell within the right of access of the claimant, however, the church was entitled to anonymize them.</p>		

Poland

Contributors



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



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

Agnieszka Sagan-Jezowska
Senior Associate
T: +48 2 25 05 07 30
agnieszka.sagan-jezowska@
eversheds-sutherland.pl

Development	Summary	Date	Links
Amended list of a kind of processing operations which are subject to the requirement for a data protection impact assessment	PUODO, the Polish DPA, published an amended list of processing operations which subject to the requirement for a data protection impact assessment ("DPIA"). The preamble to the list has changed, clarifying the need for a DPIA if at least two criteria are met. The list itself has not changed compared to the previous version of the list.	8 July 2019	DPIA list
The Public Documents Act in force	<p>The new Public Documents Act entered into force. The Act prohibits the making and trading of replicas of public documents eg of identification ("ID") or driving licenses. According to PUODO, not every copy of a public document will be prohibited, but an entity that copies, for example, an ID card may be responsible for processing too wide a range of personal data.</p> <p>In the opinion of PUODO, most entities that often make photocopies of documents of natural persons cannot justify it with such goals as, eg conclusion of a contract, potential legal claims. The most controversial was the copying of ID by banks. According to PUODO, banks cannot copy IDs eg when setting up an account, checking creditworthiness or concluding a loan agreement. The provision of Art. 112 of Banking Act entitles banks to process data contained in IDs, not to copy all of the ID documents.</p> <p>According to PUDO, making a copy of the ID is allowed for compliance with financial security measures under the Anti-Money Laundering Act. The copy of ID must be processed for the purpose of AML only.</p>	<p>12 July 2019</p> <p>1 September 2019</p>	<p>Press release</p> <p>Press release</p>



Development	Summary	Date	Links
	The PUODO consolidated its position in response to the President of The Polish Bank Association of 9 September 2019.		
Short tips on notification of data breach to the PUODO	<p>PUODO published four short tips on what to remember when the controller notifies a data breach. In addition to recalling the basic principles for reporting violations, PUODO paid special attention to the choice of the form of informing data subjects on a data breach. According to PUODO, in some cases, one form of communication is not enough and the controller should use several alternative methods, eg direct communication (e-mail, SMS), eye-catching banners, notifications on websites or advertisements in printed media.</p> <p>The document published by the PUODO is a useful summary of the controller's responsibilities in the case of a data breach.</p>	1 August 2019	Press release
Examining employees with a breathalyzer by employers is not allowed	<p>Under the Polish legal acts, there is no legal basis for employers examining employees with a breathalyzer. An employee sobriety test can only be conducted by the police, not the employer.</p> <p>The PUODO published their statement on this issue a few months ago, now the statement has been confirmed by the Ministry of Labour and Social Solidarity and Family.</p>	16 September 2019	Press release
EUR 600 000 fine imposed on morele.net in Poland	<p>The PUODO imposed the third fine under the GDPR in Poland. The fine of approximately EUR 600 000 was imposed on morele.net for insufficient organizational and technical safeguards.</p> <p>As a result of hackers attacking the servers of the company's website, the personal data of 2.2 million natural persons was disclosed. According to the PUODO, the company didn't implement appropriate procedures to react in the event of unusual network traffic.</p> <p>The imposed fine is the third financial penalty under the GDPR in Poland as well as the highest GDPR fine imposed by Polish data protection authority.</p>	19 September 2019	Press release Decision

Romania

Contributors



Mihai Guia
Managing Partner
T: +40 21 31 12 56 1
mihaiguia@
eversheds.ro



Alexandra Sulea
Senior Associate
T: +40 21 311 2561
alexandrahutar@
eversheds.ro

Development	Summary	Date	Links
July			
EUR 15,000 fine applied for lack of compliance with the security requirements and for unauthorized disclosure of personal data	The EUR 15,000 fine, the second fine applied in Romania, was issued to the World Trade Centre Hotel for failing to take the necessary measures and safeguards against unauthorized disclosure of personal data. They reported a data breach to the authority after a list with information about 46 guests who were having breakfast at the hotel was photographed by an unauthorised person and published online.	Issued: 2 July 2019	Press release
EUR 3,000 fine applied for lack of compliance with the security requirements and for unauthorized disclosure of personal data	The third fine under GDPR in Romania was of EUR 3,000 and it was applied to a website selling GDPR implementation toolkits and compliance programs. The company failed to take the necessary security measures during a platform migration, and two links to a list of files were made available for public access. The files contained business contacts of clients purchasing the GDPR toolkits – names, postal address, e-mail, phone, workplace etc.	Issued: 5 July 2019	Press release
EUR 2,500 fine for lack of information notice and for disclosure of personal identification number	The fourth fine under GDPR has been applied after a data subject submitted a complaint to the Romanian DPA regarding an entity which (i) used CCTV cameras on its premises, without informing the data subjects of such; and (ii) disclosed the names and the personal identification numbers of its employees on the company's notice board. The Romanian DPA has concluded that the entity did not comply with its information notice obligation and also, that it did not have any legal basis for the disclosure of the personal data of the employees.	Issued: July 2019	Press release



Contributors

Switzerland



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

Development	Summary	Date	Links
Limitation of employer's right to monitor employees' use of electronic devices	<p>The Court of Appeal of the Canton Zurich decided on the question: under which conditions an employer is entitled to monitor their employees' use of business mobile phones in order to ensure compliance with the company's policies. In the case at hand, the company's internal policies prohibited the private use of the business mobile phones. Furthermore, the internal policies stated that the company is entitled to monitor the employees' use of the internet, e-mail account or business mobile phone without prior warning, if there is a suspicion of violation of the internal policies. In the case at hand, the employer realised that an employee had installed WhatsApp on his business mobile phone and suspected that the employee was using WhatsApp for private purposes. Therefore, the employer monitored the content of the employee's WhatsApp chat. The Court of Appeal of the Canton of Zurich emphasised that an employer is only allowed to process personal data about its employees, if in particular the following principles are observed:</p> <ul style="list-style-type: none"> – the purpose of the data processing is the performance of the employment contract, the administration of the employment relationship or the assessment of a job candidate's suitability; – the processing of the personal data is adequate and necessary for that purpose and is carried out in good faith; and – the processing of the personal data is evident to the employee (principle of transparency). <p>The Court of Appeal concluded that the monitoring of the WhatsApp chat content constituted a breach of the employee's privacy. First of all, it was not necessary to access the content of the WhatsApp chat in order to ensure compliance with the company's policies. In general, accessing the content of employees' private messages can only be lawful in exceptional cases. Secondly, the provision in the internal policies, which stated that the company is entitled to monitor the employees' use of the internet, e-mail account or business mobile phone without</p>	Decision: 20 March 2019	N/A



Development	Summary	Date	Links
	<p>prior warning if there is a suspicion of violation of the internal regulations, was considered to be too vague, because the employees need to have a clear understanding of when and under which conditions the company may monitor the use of electronic devices. Finally, the Court of Appeal pointed out that an employee cannot validly consent to a data processing not necessary for the purpose mentioned above. Hence, even with the employee's consent, the employer would not have been allowed to access the content of the WhatsApp chat.</p>		





United Kingdom

Contributors



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



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

Development	Summary	Date	Links
New guidance on cookies from ICO	<p>On 3 July, the Information Commissioner's Office ("ICO") then published their revised guidance on the use of cookies. The guidance examines the use of cookies and similar technologies (including device fingerprinting identifiers) in detail and explains, among other things, that:</p> <ul style="list-style-type: none"> – unless an exemption applies, any use of cookies requires the provision of clear and comprehensive information - which means you must provide the same kind of information to users as you would do when processing their personal data. The information must include the types of cookies you intend to use, and the purposes for which you intend to use them; – you cannot rely on implied consent for cookies. Any non-essential cookies, including third party cookies used for the purposes of online advertising or web analytics, require prior consent to the GDPR standard; – analytics cookies are not "strictly necessary" because they are not part of the functionality that the user requests when they use the relevant online service; – users must be provided with free choice; consent should not be bundled up as a condition of service unless it is necessary for that service. In its blog post, the ICO acknowledges there are some differing opinions as well as practical considerations around the use of partial cookie walls and confirms it will be seeking further submissions and opinions on this point from interested parties; and – legitimate interests cannot be relied on for the setting of cookies - PECR always requires consent for cookies, unless an exemption applies. <p>In its accompanying blog post, the ICO warns that cookie compliance "will be an increasing regulatory priority for the ICO in the future" but that "any future action would be proportionate and risk-based". Organisations are</p>	3 July 2019	Guidance Blog post



Development	Summary	Date	Links
	recommended to start working towards compliance now, by undertaking a cookie audit and documenting decisions.		
CMA launches digital markets strategy and market study into online platforms and digital advertising	<p>The Competition and Markets Authority (“CMA”) launched a market study into online platforms and the digital advertising market in the UK.</p> <p>The CMA is looking at three broad potential sources of harm to consumers in connection with the market for digital advertising:</p> <ul style="list-style-type: none"> – to what extent online platforms have market power in user-facing markets, and what impact this has on consumers; – whether consumers are able and willing to control how data about them is used and collected by online platforms; and – whether competition in the digital advertising market may be distorted by any market power held by platforms. <p>Comments were due in by 30 July 2019, including from interested parties such as online platforms, advertisers, publishers, intermediaries within the ad tech stack, representative professional bodies, government and consumer groups.</p>	3 July 2019	CMA statement Statement of scope
ICO annual report 2018-19	<p>The ICO published their 2018-19 report. The report notes the following highlights:</p> <ul style="list-style-type: none"> – the ICO’s helpline, chat and written advice services received 471,224 contacts in 2018-19, a 66% increase from 2017/18 (283,727 contacts); – data protection complaints received by the ICO increased from 21,019 in 2017/18 to 41,661 in 2018/19; – preparation of statutory codes focusing on age appropriate design, data sharing, direct marketing, and data protection and journalism; – using new powers of inspection - issuing 11 assessment notices in conjunction with our investigations into data analytics for political purposes, political parties, data brokers, credit reference agencies and others; and – issuing warnings and reprimands across a range of sectors including health, central government, criminal justice, education, retail and finance. 	9 July 2019	ICO statement



Development	Summary	Date	Links
ICO blog: Live facial recognition technology – data protection law applies	<p>The Information Commissioner published a blog post on live facial recognition (“LFR”) technology. The blog post explains how extensive use of LFR represents the widespread processing of biometric data of thousands of people as they go about their daily lives.</p> <p>The ICO is conducting an investigation, monitoring the trials carried out by the police deploying this technology. The Commissioner highlights the case - R (Bridges) v Chief Constable of South Wales Police (SWP) – which involves a member of the public who has concerns that his image may have been captured on LFR from a police van while he was out shopping in Cardiff city centre. He has brought the case, to ask the courts to decide whether the use of facial recognition in this way by SWP is lawful.</p>	9 July 2019	ICO blog post
Centre for Data Ethics and Innovation interim reports on reviews into online targeting and bias in algorithmic decision-making	<p>The Centre for Data Ethics and Innovation (“CDEI”) (an independent advisory body, led by a board of experts, set up and tasked by the UK Government to investigate and advise on how we maximise the benefits of data-driven technologies) published two interim reports on its major reviews into online targeting and bias in algorithmic decision-making.</p> <p>The report on the review into online targeting reveals that the CDEI’s work to date has led to the following insights:</p> <ul style="list-style-type: none"> – people’s attitudes towards targeting change when they understand more of how it works and how pervasive it is - while people recognise the benefits of online targeting, most seem to agree that there are some forms of targeting which make them uncomfortable, and that changes are needed to the way targeting is practised and overseen; – any changes to oversight mechanisms need to take into account how responsibility should be split between different actors, how to make the most of market incentives, voluntary regulation and empowering users, and how to enable effective monitoring and enforcement; and – potential solutions could include stronger regulations, greater transparency and visibility of how targeting operates, giving individuals stronger controls or rights over how data about them is used. <p>The report on the review into bias in algorithmic decision-making summarises that:</p> <ul style="list-style-type: none"> – the tension between the need to create algorithms which are blind to protected characteristics, while also checking for bias against those same 	19 July 2019	Press release Interim report on review into online targeting Interim report on review into bias in algorithmic decision making



Development	Summary	Date	Links
	<p>characteristics, creates a challenge for organisations seeking to use data responsibly;</p> <ul style="list-style-type: none"> – new approaches to identifying and mitigating bias are required - specific tools are already starting to be developed but there is limited understanding of the full range of tools and approaches available (current and potential) and what constitutes best practice, which makes it difficult for organisations that want to mitigate bias in their decision-making processes to know how to proceed and which tools and techniques they should use; and – effective human accountability for the use and performance of algorithmic tools will be critical and tools must be used as part of a system of governance that is demonstrably trust-worthy - this may require new functions and actors, such as third party auditors, to independently verify claims made by organisations about how their algorithms operate. The CDEI will take a sector approach to test their hypotheses and explore what is required to operationalise ethical approaches in practice. 		
ICO launches updated data sharing code of practice for consultation	<p>The ICO has launched a consultation on its updated data sharing code of practice. The consultation closes on 09 September 2019.</p> <p>The updated code replaces a 2011 code, as required under the Data Protection Act 2018. The code explains changes to data protection legislation where relevant to data sharing.</p> <p>For a summary of the draft code, you can read our briefing here.</p>	16 July 2019	Consultation Eversheds Sutherland briefing
NCSC publishes second Active Cyber Defence report	<p>The National Cyber Security Centre ("NCSC") has published its second report examining how its Active Cyber Defence ("ACD") programme is improving the security of the UK public sector and the wider UK cyber ecosystem. The report concludes that the programme, which aims to mitigate the harm caused by cyber-attacks against the UK, has had a positive impact, but that there is still room for improvement.</p> <p>The report assesses developments in the following ACD programme services:</p> <ul style="list-style-type: none"> – takedown service - removing malicious content from the internet; – mail check - helping domain owners understand and control abuse of their email domains; 	16 July 2019	Report Blog post



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – domain discovery - helping system owners understand what internet domains they have registered; – web check - proactively scanning websites for vulnerabilities and issues; – protective Domain Name System - protecting the public sector at scale from harmful internet threats; – routing and signalling - protecting the protocols that route internet traffic; – host-based capability - understanding public sector IT; – vulnerability disclosure platform - streamlining the report process for vulnerabilities in government services; and – suspicious email incubator - building a service to help the public report suspicious internet incidents and activity and automatically taking protective action. 		
Select Committee response to Government's Online Harms White Paper	<p>The House of Commons' Digital, Culture, Media and Sport Committee ("Committee") responded to the Government's White Paper on Online Harms which was published in April 2019 (shortly after the Committee's own report on disinformation and fake news in February 2019).</p> <p>In summary, the Committee is pleased that the government has taken up a large number of its recommendations; in particular, proposals to establish an independent regulator for online harms and to require social media companies to comply with a 'duty of care'.</p> <p>However, the Committee considers that a "significant gap" exists between their recommendations and White Paper in that there is little focus on electoral interference and online political advertising, which it highlighted in its report as needing urgent action.</p> <p>The Committee accuses the Government of ignoring the recommendations contained in the Committee's final report into Disinformation and "fake news", including the following:</p> <ul style="list-style-type: none"> – introduce a new category for digital spending on political campaigns; – ensure information about all online political advertising material is logged in a searchable public repository; – acknowledge the risks of foreign investment in elections, for example via digital payments; and 	2 July 2019	DCMS Committee statement DCMS Committee report on Online Harms White Paper ICO response to white paper Government White Paper on Online Harms



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – acknowledge the role and power of unpaid campaigns and Facebook Groups in influencing elections and referendums, inside and outside the designated period. <p>The Committee notes that in a separate paper, Elizabeth Denham (the Information Commissioner) also expressed surprise and disappointment that the white paper did not contain more on electoral interference and transparency in political advertising.</p>		
Government consults on new plans to make online identity verification safer	<p>The Government has launched a call for evidence, seeking views on how to improve the ways people and organisations can digitally verify identities.</p> <p>According to the corresponding press release, the call for evidence will explore the role of government and the private sector in the development of digital identities – the way people prove they are who they say they are using digital technology – and seek views on how to achieve higher levels of trust between the public and organisations checking their identities.</p> <p>The proposals aim to help make verification methods quicker, easier and more secure – in particular, to reduce the opportunity for fraud.</p> <p>The consultation closes on 15 September 2019.</p>	19 July 2019	Press release Consultation
Government guide on how to help customers better understand contractual terms and privacy policies	<p>The Department for Business, Energy & Industrial Strategy (“BEIS”) has published a guide for businesses on how to help customers better understand contractual terms and privacy policies.</p> <p>The guide looks at various techniques for improving consumers’ understanding of contractual terms, conditions and privacy policies while focusing on methods offering low-cost and scalable solutions. Techniques found to be particularly effective at improving understanding, include:</p> <ul style="list-style-type: none"> – displaying key terms as frequently asked questions; – using icons to illustrate key terms; – showing customers your terms within a scrollable text box instead of requiring a click to view them; – providing information in short chunks at the right time; and – using illustrations and comics. <p>The literature review, which accompanies the guide, summarises existing evidence on techniques to increase consumer engagement with, and</p>	18 July 2019	Best practice guide Literature review Technical report Press release



Development	Summary	Date	Links
	understanding of, online contractual terms and privacy policies. In addition, a technical report details the six experiments conducted by the Behavioural Insights Team (the company engaged by BEIS to conduct the research) for the study.		
ICO selects first participants for data protection Sandbox	<p>The ICO has published details of the first participants to its data protection Sandbox initiative.</p> <p>The sandbox is a new ICO service which supports organisations developing innovative products and services using personal data with a clear public benefit. According to the ICO, “participants will be able to draw on the ICO’s expertise and advice on data protection by design, mitigating risks as they test their innovations, while ensuring that appropriate protections and safeguards are in place”.</p> <p>The first projects to take part in the Sandbox involve the use of biometrics to speed up airport passenger journeys, innovations in crime prevention and technological advances in the health sector.</p> <p>The ICO has said previously that it hopes to treat the Sandbox projects “as use-cases to anticipate change and develop public guidance and resources on compliance, and potentially to feed into the development of codes of conduct in particular sectors where future regulatory provision may be required”.</p>	29 July 2019	Press release
Association of British Insurers calls for ICO to reveal cyber data	<p>The Association of British Insurers (“ABI”) has repeated its call for the ICO to share anonymised cyber breach data and make it publicly available, to enable insurers price risk more accurately and manage exposure more effectively by feeding that data directly into their modelling.</p> <p>According to the statement, the ABI “will continue to work with the ICO to find a solution that enables both innovation and data privacy in the Cyber market”.</p>	8 August 2019	ABI statement
FCA agrees plan for a phased implementation of Strong Customer Authentication	<p>The FCA has agreed a plan giving the payments and e-commerce industry extra time to implement Strong Customer Authentication (“SCA”) rules which will apply from 14 September 2019.</p> <p>The FCA has agreed an 18-month phased plan to implement SCA with the e-commerce industry of card issuers, payments firm and online retailers, which reflects the recent opinion of the European Banking Authority.</p> <p>The FCA confirmed it “will not take enforcement action against firms if they do not meet the relevant requirements for SCA from 14 September 2019 in areas covered by the agreed plan, where there is evidence that they have taken the</p>	13 August 2019	FCA press release



Development	Summary	Date	Links
	necessary steps to comply with the plan. At the end of the 18-month period, the FCA expects all firms to have made the necessary changes and undertaken the required testing to apply SCA".		
Information Commissioner blogs about what aspects people are most concerned about	The Information Commissioner, Elizabeth Denham, published a blog post commenting on the issues people have indicated are most concerning them. The Commissioner cited the Information Commissioner's Office's ("ICO") recent annual track survey which highlighted cyber security as top of the list of concerns. Children's privacy and data sharing were also high on the list. She also noted that responses to the survey show a decline in public confidence in the ability of companies and other organisations to store and use personal information.	31 July 2019	Blog post Trust and confidence survey
New High Court List for data protection claims	<p>The Civil Procedure Rules ("CPR") have been updated to include a new Part 53 CPR, which requires all High Court data protection claims issued after 1 October 2019 to be issued in the new Media and Communications List of the High Court. Two new Practice Directions have also been published, along with a corresponding Pre-Action Protocol which sets out what should be included in the Letter of Claim for data protection cases.</p> <p>Notably, the new Practice Direction 53B specifies the following in respect of data protection claims:</p> <p>9. In any claim for breach of any data protection legislation the claimant must specify in the particulars of claim—</p> <p>(1) the legislation and the provision that the claimant alleges the defendant has breached;</p> <p>(2) any specific data or acts of processing to which the claim relates;</p> <p>(3) the specific acts or omissions said to amount to such a breach, and the claimant's grounds for that allegation; and</p> <p>(4) the remedies which the claimant seeks.</p>	18 July 2019	Civil Procedure Rules website Civil Procedure (Amendment No. 3) Rules 2019 schedule Practice Directions 53A and 53B Pre-Action Protocol for Media and Communication Claims
Online child protection code update	In a blog post, the Information Commissioner provided an update on the development of a new code of practice to protect children online. The ICO has received 450 written responses to the consultation which took place from 12 April to 31 May 2019. The final code is due to be delivered before the 23 November statutory deadline. In her blog, the Commissioner emphasised the ICO's "aim has never been to keep children from online services, but to protect them within it" and that it wants "providers to set their privacy	7 August 2019	Blog post Draft "Age appropriate design: a code of practice for online services" for consultation



Development	Summary	Date	Links
	settings to 'high' as a default, and to have strategies in place for how children's data is handled".		
ICO issues draft framework code of practice for the use of personal data in political campaigning	<p>Following an initial call for views late last year, the ICO has released a draft code of practice for the use of personal data in political campaigning. The code does not introduce new requirements for campaigners but aims to explain and clarify current data protection and electronic marketing laws as they apply to political campaigning. It is hoped that the code will provide practical guidance and useful examples on ways campaigners can comply with their obligations whilst carrying out common political campaigning activities. In its statement, the ICO noted that the code "has the potential to become a statutory code of practice if the relevant legislation is introduced". The consultation closes on 4 October 2019.</p>	9 August 2019	Consultation details Draft framework code BBC article
Safeguarding personal data in automated artificial intelligence systems	<p>Another blog post in the ICO's ongoing call for input on developing its framework for auditing AI, outlines some of the key safeguards organisations should implement when using solely automated AI systems to make decisions with significant impacts on data subjects. The blog post draws on guidance issued by the EDPB on automated individual decision-making and profiling under GDPR.</p> <p>In order to help address the risks that machine learning systems pose to people's data protection rights, the ICO recommends that organisations should:</p> <ul style="list-style-type: none"> – consider the system requirements necessary to support a meaningful human review from the design phase. Particularly, the interpretability requirements and effective user-interface design to support human reviews and interventions; – design and deliver appropriate training and support for human reviewers; and – give staff the appropriate authority, incentives and support to address or escalate data subjects' concerns and, if necessary, override the AI system's decision. <p>In addition, organisations should consider:</p> <ul style="list-style-type: none"> – the need for a data protection impact assessment before using solely automated systems to make decisions with legal or significant effects on data subjects; 	5 August 2019	ICO blog post



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – safeguards for solely automated AI systems to be designed holistically and with the data subject in mind; – that the information about the logic of a system and explanations of decisions should give data subjects the necessary context to decide whether, and on what grounds, they would like to request human intervention; – the process for data subjects to exercise their rights should be simple and user friendly; and – monitoring and analysing whether and how data subjects exercise their rights in relation to automated decisions and amend their systems and processes accordingly. 		
Data Protection Act 2018 (Commencement No. 2) Regulations 2019 SI 2019/1188 made	The Regulations bring into force the remaining provisions of Part 4 of the Data Protection Act 2018, which relates to data processing by the Intelligence Services, so far as they were not already in force. The provisions will come into force in the UK on 16 September 2019. The provisions are s93, ss102-105 and s108 of the DPA 2018.	5 August 2019	Legislation
ICO investigates Kings Cross use of facial recognition	<p>The Information Commissioner issued a statement in response to reports on the use of facial recognition technology ("FRT") in the Kings Cross area. The Commissioner notes that FRT is a "priority area for the ICO and when necessary, we will not hesitate to use our investigative and enforcement powers to protect people's legal rights". The ICO has launched an investigation following the concerns reported in the media – the investigation will require the relevant organisations to submit detailed information about how the FRT is used and the ICO will also conduct an on-site inspection of the system to assess its compliance.</p> <p>The Commissioner highlighted her concerns over the growing use of FRT in a blog post earlier this summer in relation to ongoing trials of the technology being conducted by various police forces.</p>	15 August 2019	ICO statement BBC article
ICO updates guidance on individuals' rights	The ICO has updated their guidance on how to calculate the time limit for responding to requests (in relation to individual rights to bring its approach in line with that taken across the EU and adopted by the EDPB. The effect is that the timescale for responding to individuals' requests (including subject access requests) is one calendar month from the day of receipt of the request, not the day after receipt. Read our briefing here .	15 August 2019	Eversheds Sutherland briefing (timescales) Eversheds Sutherland briefing (manifestly



Development	Summary	Date	Links
	In addition, the ICO has added guidance on the meaning of “manifestly unfounded or excessive” in relation to requests from individuals to exercise their rights. Read our briefing here .		unfounded or excessive) ICO statement What's New section of ICO guidance
ICO blogs about techniques for data minimisation in AI Systems	<p>As part of an ongoing consultation into developing a framework for auditing AI, the ICO published a blog post about how organisations which use AI systems can ensure compliance with the ‘minimisation principle’ under data protection law. This principle requires entities to only process personal data which is ‘adequate, relevant and limited to what is necessary’. This criteria tends to be case-specific.</p> <p>The ICO recommends techniques which could be adopted to minimise the amount of data an organisation needs to process. The blog focuses on supervised Machine Learning (“ML”) systems, which are currently the most commonly used type of AI.</p> <p>The recommended techniques include the following:</p> <ul style="list-style-type: none"> – modification of training data by changing values of an individual’s data points to add ‘noise’ to the data and reduce the extent to which it is traceable to a specific person; – converting ‘human readable’ words into abstract number sequences so that there is no need to process human-interpretable versions of personal data; – hosting ML models on a user’s device to make inferences ‘locally’, rather than on a cloud server; and – reducing the amount of data revealed in a query sent to ML models by retrieving predictions or classifications without disclosing all the information to the party running the model. 	21 August 2019	ICO blog
Over £900,000 confiscated from cyber hacker	A hacker who carried out cyberattacks on more than 100 companies worldwide has been subjected to a confiscation order for £922,978.14 of cryptocurrency under the Proceeds of Crime Act 2002. The cybercriminal, who was identified as head of an Organised Crime Network, used ‘phishing’ emails to obtain customers’ financial data to sell on the dark web and convert the profit into cryptocurrency.	23 August 2019	Met police statement



Development	Summary	Date	Links
Create access to traffic data and deploy AI to help end traffic congestion and pollution says Department for Transport	<p>Following a review of legislation on traffic regulation orders (“TROs”) – orders which permit temporary or permanent changes to roads – the Department for Transport has announced plans to create access to data on planned changes to road networks.</p> <p>By opening up TRO data, there is the potential for companies to develop navigational apps powered by AI which could allow road users to be warned of disruptions months in advance, thereby decreasing congestion and pollution.</p> <p>The review supports the government’s Future of Mobility Grand Challenge which assesses whether current legislation is able to maximise the potential of future technologies, such as self-driving vehicle technology in this case.</p>	26 August 2019	Department for Transport press statement
Department for Education updates guidance on Privacy Notices	<p>The Department for Education (“DfE”) has updated the suggested privacy notices templates for use by schools and local authorities to issue to individuals including staff, parents and pupils about the collection of personal data.</p> <p>DfE also amended its user guidance to highlight the need for parental consent to share any additional pupil information with local authorities and youth support services.</p>	21 August 2019	Statement (including suggested text) Guidance
High Court rules that police use of automated facial recognition technology is lawful	<p>In R (on the application of Bridges) v Chief Constable of South Wales Police (Information Commissioner and another intervening), the High Court issued its verdict on the use of Automated Facial Recognition (“AFR”) in reportedly the first judgment of its kind by any court in the world. The case was brought by a civil liberties campaigner (‘the claimant’) who sought judicial review of an AFR pilot project called ‘AFR Locate’ by the South Wales Police (“SWP”). AFR Locate uses digital video footage from surveillance cameras to isolate images of individual faces, extract biometric data and identify likely matches against a database.</p> <p>The claimant argued that SWP’s use of AFR Locate infringed his right to a private life under the Human Rights Act 1998 (“HRA”) and failed to comply with the principle that personal data must be processed fairly and lawfully under the Data Protection Act 1998 (“DPA 1998”).</p> <p>The application for judicial review was dismissed on the grounds that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR technology. The High Court also found that the processing of personal data by SWP was lawful, not disproportionate and met all the conditions required by both the HRA and DPA. It was decided that SWP has</p>	4 September 2019	Judgment ICO statement SCC press release SCC statement



Development	Summary	Date	Links
	<p>sufficient legal controls and appropriate privacy safeguards in place. Yet the High Court's decision was case-specific and it is unlikely to prevent further questions over the use of AFR by local authorities in the future.</p> <p>The ICO announced that it will use the High Court's findings to finalise its guidance for police forces on the deployment of AFR technology.</p> <p>In addition, the Surveillance Camera Commissioner ("SCC") released a statement warning that the judgment ought not to be interpreted as a green light for the deployment of AFR generally and emphasising the need for it to be used within the legal framework, having regard to good governance and legitimacy of endeavour.</p>		
ICO warns against retention of personal data accessed through work	<p>The ICO issued a warning against knowingly or recklessly retaining personal data obtained in the course of employment, without the consent of the data controller. This is now a criminal offence under the Data Protection Act 2018 ("DPA 2018"). The ICO advises anyone who deals with personal data during the course of their work to be aware of the DPA 2018, particularly upon retiring or taking a new job.</p>	5 September 2019	ICO statement
CMA publishes responses to study on digital advertising and online platforms	<p>As part of a market study into online platforms and digital advertising in the UK, the Competition and Market Authority ("CMA") invited responses to detailed issues set out in a Statement of Scope. The CMA published the comments it received from 57 respondents including social media platforms (eg Google and Facebook), advertisers (eg L'Oréal), publishers (eg The Guardian), representative industry bodies (eg IAB UK), consumers, software developers and picture libraries.</p> <p>The respondents encourage a cautious approach to market intervention. The following are some of observations made by respondents:</p> <ul style="list-style-type: none"> – advantages of digital advertising include better focus and stability for advertisers and free services and less irrelevant advertising for consumers; – constant innovation and new technologies are likely to heighten the tough competition which is already present in the sector; – exaggeration of the benefits of large datasets collected by big platforms should be avoided, given the availability of third-party data; and 	11 September 2019	CMA webpage



Development	Summary	Date	Links
	<ul style="list-style-type: none"> the advertising industry should address the market dominance of large platforms and ensure that consumers have control over the use of their data. <p>The respondents have advocated that the CMA should use their intel to formulate potential remedies. The CMA is expected to publish a final report by 2 July 2020.</p>		
ICO guidance on how SMOs can prepare for a no-deal Brexit	<p>The ICO issued guidance to help small and medium sized organisations (“SMOs”) prepare for a potential no-deal Brexit. The guidance includes steps on how to maintain data flows, for example using the pre-approved standard contractual clauses which are already being used to transfer personal information internationally.</p> <p>Any UK organisations with an established presence or customer base in the EEA will have to comply with both UK and EU data protection regulations after Brexit, meaning businesses may need to designate a representative in the EEA.</p>	11 September 2019	ICO statement Guidance
ICO blogs about new privacy and security risks in AI	<p>In a recent blog post, the ICO has highlighted privacy and security risk associated with the use of AI and ML, whereby the personal data of the people who the system was trained on might be revealed by the system itself – such risks include ‘model inversion’ and ‘membership inference’ attacks.</p> <p>‘Model inversion’ is possible if the attackers already have access to certain personal data about particular individuals included in the training data, they can infer further personal information about those individuals by observing the inputs and outputs of the ML model. In a ‘membership inference’ attack, malicious actors are able to deduce whether a specific individual was present in the training data of a ML model.</p> <p>The ICO’s AI team make a number of recommendations, including that organisations which train models and provide them to others should assess whether those models might contain personal data, or whether they are at risk of revealing it if attacked. In addition, organisations should stay up to date with the state of the art in methods of attack and mitigation.</p>	12 September 2019	ICO blog post
Centre for Data Ethics and Innovation publishes first paper on ethical issues in AI	<p>The Centre for Data Ethics and Innovation (“CDEI”) published its first series of three snapshot papers on ethical issues in AI. The three papers cover the following topics:</p> <ul style="list-style-type: none"> deepfakes and audiovisual information (22 pages) 	12 September 2019	CDEI papers



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – smart speakers and voice assistants (27 pages) – AI and personal insurance (28 pages) <p>The objective of the papers is to improve the understanding of topical issues related to the development and deployment of AI.</p>		
DCMS Select Committee reports on immersive and addictive technologies	<p>The House of Commons DCMS Select Committee published a report on immersive and addictive technologies, the product of an inquiry involving players from the gaming and social media industries. The report contains a number of recommendations for the Government to consider, including:</p> <ul style="list-style-type: none"> – the sale of loot boxes to children should be banned; – the Government should regulate 'loot boxes' under the Gambling Act; – an industry levy should be set up to support independent research into the effects of gaming; and – the games industry must face up to responsibilities to protect players from potential harms. <p>The committee also expressed serious concern at the lack of an effective system to keep children off age-restricted platforms and games. Many participants in the enquiries that fed into the report did not have in place robust systems to verify users' age, despite the GDPR applying specific protections obligations in respect of the processing of children's personal data.</p>	12 September 2019	Committee statement Report
DCMS call for views on cyber security certification post-Brexit	<p>The Department for Digital, Culture, Media & Sport ("DCMS") launched a consultation calling for views on the proposed approach to cyber security certification following the UK's exit from the EU. The recently enforced EU Cyber Security Act established a cyber security certification framework for EU-wide implementation. The UK wants to negotiate a mutual recognition agreement with the EU to maintain its close cyber security relationship following Brexit. The consultation closes on 8 October 2019.</p>	12 September 2019	DCMS call for views
Ofgem seeks feedback on draft cyber resilience guidance	<p>Ofgem is seeking feedback on its draft Cyber Resilience guidance documents, to assist in RIIO-2 Operational Technology Cyber Resilience planning.</p> <p>RIIO stands for Revenue = Incentives + Innovation + Outputs. It is Ofgem's performance-based framework to set price controls.</p> <p>The guidance is designed to assist in RIIO-2 Operational Technology Cyber Resilience planning, based on the NCSC sector-agnostic Cyber Assessment</p>	13 September 2019	Ofgem consultation



Development	Summary	Date	Links
	<p>Framework ("CAF"). The feedback received will be considered for inclusion in a subsequent version of the guidance which will also incorporate changes arising from the NCSC CAF review.</p> <p>The deadline for responses was 11 October 2019.</p>		
Claimant granted injunction to prevent processing of personal data in defamatory videos	<p>In <i>Al-Ko Kober Ltd and another v Sambhi</i> [2019] EWHC 2409 (QB), the High Court allowed a summary judgment and granted a final injunction in respect of claims for defamation, breach of the Data Protection Act 1998 ("DPA 1998") and malicious falsehood.</p> <p>The first claimant was a subsidiary of a German registered company and the second claimant was that company's Marketing Manager. The first claimant and the defendant both manufacture caravan towing stabilisers in competition with one another. The defendant had published a number of Youtube videos, which among other things, portrayed the first claimant's products as unsafe and that the claimants were operating a fraudulent business. The videos also included footage of the second claimant speaking at trade shows. The second claimant brought claims alleging that the defendant's processing breached the first data protection principle of the DPA 1998 in that it was defamatory of the second claimant and lacked a lawful basis and that the processing caused him substantial and unwarranted damage and distress. He called for the defendant's processing to be prevented by a court order made under section 10(4) of the DPA 1998 and he claimed damages under section 13 of the DPA 1998.</p> <p>The court held that the videos contained the second claimant's personal data and that the processing was unlawful on the basis that no Schedule 2 condition applied to the processing. However, the judge did not make a conclusion as to whether the processing breached the first data protection principle, finding that it was "not appropriate for it to be determined on an application for summary judgment" (– the claimant's submission had been that any act of defamation involving the processing of personal data must also contravene the requirements of the DPA 1998).</p> <p>The court also left the issue of the claim for damages under s13 DPA 1998 to be considered at a further hearing.</p>	13 September 2019	Judgment
NCSC paper on cyber threats to UK universities	<p>The NCSC has published a paper which examines the cyber security threat to UK universities - including who is targeting the sector, why their attacks may be successful and a look at the future of the threat.</p>	18 September 2019	NCSC paper



Development	Summary	Date	Links
	<p>The paper concludes that the key cyber threats are likely to be:</p> <ul style="list-style-type: none"> – criminals seeking financial gain; and – nation states looking to steal personal data and intellectual property, for strategic advantage. <p>According to the paper, the kinds of data and information of interest to a nation state could include:</p> <ul style="list-style-type: none"> – emails; – bulk personal information on staff and students; – technical resources (eg documentation and standards); and – sensitive research and intellectual property. 		
BEIS report recommends UK to develop robots and AI strategy	<p>The House of Commons Department for Business, Energy and Industrial Strategy (“BEIS”) Select Committee have published a report which reflects on the UK’s ‘slow place in moving to automation’.</p> <p>In the report, the Committee calls upon the Government to develop a UK Robot and AI Strategy to support businesses and workers as they manage the transition to a more automated world of work, and to work with universities and businesses to provide advice, networking, and access to finance necessary for the UK to “reap the benefits of domestic tech success stories rather than too often seeing these businesses get snapped up by overseas investors”.</p> <p>The report finds that a ‘robot tax’ would discourage take up of automation and that it would not be in the interest of businesses or workers in the UK.</p> <p>The report also recommends the Government brings forward proposals for a new tax incentive to encourage investment in new technology, such as automation and robotics.</p> <p>The report notes the risk that the transition to a more automated workplace and society could lead to a reduction in the quality of work, widening existing inequalities and increasing regional disparities and finds the lack of planning in this area “worrying” given the Government’s role in education, regional and business policy. The report recommends that the Government supports those most affected and provides local areas with the support and incentives needed to enable the transition.</p>	18 September 2019	Press statement Report



Development	Summary	Date	Links
NCSC guidance on cyber incident management	<p>The NCSC issued guidance on cyber incident management, to help organisations plan, build, develop and maintain an effective cyber incident response capability.</p> <p>The guidance comprises of the following:</p> <ul style="list-style-type: none"> – an introduction to the incident response process, including the important issues of detection and notification; – an outlines of the ingredients of a basic response plan; – advice on how to form an incident response team, including the skillsets and roles required; – guidance on the tools and technology required in the event of a cyber security incident; and – considerations when designing, building and maintaining your Incident Response (IR) capability. 	19 September 2019	Guidance
Bank of England publish findings from sector cyber resilience exercise	<p>The Bank of England published the high level findings of SIMEX18 – a 2018 sector wide cyber simulation exercise – took place on 9 November 2018.</p> <p>The exercise found the following:</p> <ul style="list-style-type: none"> – there are opportunities to improve the way firms coordinate at an operational level during incidents that impact the sector; – there is disparity in risk tolerance for suspending services could impact the functioning of the financial sector; – the recovery of services is impacted by differences in the way data is stored across the financial sector; and – effective and consistent communications are key to maintaining customer and market confidence. 	27 September 2019	Statement Report

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
July			
The Cryptography Law of the People's Republic of China (中华人民共和国密码法 (草案))	<p>On 5 July 2019, the Standing Committee of the National People's Congress released a new draft of the Cryptography Law of the People's Republic of China which details the requirements for commercial cryptography products relating to cybersecurity. These requirements include the following provisions:</p> <ul style="list-style-type: none"> – all commercial cryptography products which involve national security, the national economy, people's livelihoods, or the public interest will be required to pass a security certification by a qualified institution in mainland China before they can be sold or supplied; – a catalogue of the relevant network key equipment and special network security products is to be compiled; and – if a critical information infrastructure operator or a government department procures and uses network products and services which involve commercial cryptography and may affect national security, a national security review organised by the cyberspace authority of the relevant state will be required in relation to such procurement and use. 	<p>Published: 5 July 2019</p> <p>Effective: Draft</p>	Link (Chinese)
Basic Specification for Collecting Personal Data via Mobile Internet Applications	On 8 August 2019, the National Information Security Standardization Technical Committee released a draft of the Basic Specification for Collecting Personal Data via Mobile Internet Applications (the "Specification"), which	Published: 8 August 2019	Link (Chinese)



Development	Summary	Date	Links
(信息安全技术 移动互联网应用 (App) 收集个人信息基本规范 (草案))	<p>clarifies that app operators need to satisfy certain basic requirements when collecting personal data.</p> <p>The Specification provides a clear definition of 'minimum scope of personal data' in Article 3.4 and gives detailed examples in its appendix.</p> <p>In addition, the Specification states that app operators will be responsible for the collection of personal data through third-party codes and plug-ins, and the app operator is required to take steps to prevent such third-party codes and plug-ins from collecting irrelevant personal data.</p>	Effective: Draft	
Regulations on the Cyber Protection of the Personal Data of Children (儿童个人信息网络保护规定)	<p>On 22 August 2019, the Cyberspace Administration of China enacted the final version of the Regulations on the Cyber Protection of the Personal Data of Children, which will come into effect on 1 October 2019.</p> <p>The main amendments reflected in the final version, which varies the draft of 31 May 2019, include:</p> <ul style="list-style-type: none"> – further emphasising that guardians should educate and guide their children on how to protect their personal data; – withdrawing certain requirements placed on DPOs in relation to privacy policies for the personal data of children; – reducing the circumstances under which a network operator may jointly use or share the personal data of children with third parties; and – removing the circumstances under which a network operator may collect the personal data of children without the consent of the child's guardian. 	Published: 22 August 2019 Effective: 1 October 2019	Link (Chinese)
Regulations relating to the Ecology of Internet Governance (Draft for Comment) (网络生态治理规定 (征求意见稿))	<p>On 10 September 2019, the Cyberspace Administration of China published a draft of the Regulations relating to the Ecology of Internet Governance (Draft for Comment) (the "REIG").</p> <p>The REIG aim to govern content distributed via the internet and to specify the scope of network information that should not be made available on the internet. The REIG also outline the duties and obligations of: online content producers, online platform operators, and internet users. In particular, online platform operators will be obliged to monitor and review the content presented on the platform and if necessary, to correct any inappropriate improper content. The Cybersecurity Administration of China may give warnings, make orders for the rectification of offending content, and impose</p>	Published: 10 September 2019 Effective: Draft	Link (Chinese)



Development	Summary	Date	Links
	penalties to the online platform producers in accordance with PRC Cybersecurity Law, if they fail to fulfil their obligations.		

Hong Kong

Contributors



John Siu
Partner
T: +852 2186 4954
johnsiu@
eversheds-sutherland.com



Jennifer Van Dale
Partner
T: +852 2186 4945
jennifervandale@
eversheds-sutherland.com



Cedric Lam
Partner
T: +852 2186 3202
cedriclam@
eversheds-sutherland.com



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



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



Aaron Hulston
Senior Associate
T: +852 2186 4919
aaronhulston@
eversheds-sutherland.com

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

Development	Summary	Date	Links
Privacy Commissioner responds to recent doxxing and cyberbullying cases	<p>In response to the recent doxxing and cyberbullying cases in Hong Kong, the Privacy Commissioner for Personal Data has brought to the public's attention potential criminal offences.:</p> <p>Under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), if a person discloses the personal data about a data user without their consent and:</p> <ul style="list-style-type: none"> – with an intention to gain or cause loss to the relevant data subject; or 	September 2019	Media statement Media statement



Development	Summary	Date	Links
	<ul style="list-style-type: none"> – regardless of a person's intent, causes psychological harm to a data subject <p>an offence is committed under the PDPO and the offender is liable to a maximum fine of HK\$1 million and 5 year imprisonment.</p> <p>Doxxing is the internet-based practice of researching and broadcasting private, personal data about an individual or organization. Doxxing activities may also involve other criminal offences like criminal intimidation.</p> <p>The Commissioner expressly stated that online platform account holders who upload personal data onto the platforms are regulated by PDPO if they control, hold, process or use the personal data from or within Hong Kong, even where such online platforms are websites registered outside Hong Kong.</p> <p>The Commissioner has been referring doxing cases to the police for criminal investigation and consideration for prosecution, and has urged online platforms to remove and suspend uploading doxxing posts.</p>		
High Court action related to a doxxing case	<p>A company and its employees have jointly filed a writ in the High Court against unnamed defendants who are only described in the writ as "persons unlawfully disclosing personal data of the first plaintiff's employees".</p> <p>The plaintiffs claimed against the defendants for damages, an injunction directing them to remove the online posts disclosing personal data, and an injunction prohibiting them from disclosing or helping others to disclose personal data of the company's employees. The personal data involved included the employees' job titles, residential addresses, the company's business address, email addresses, dates of birth, telephone numbers, Facebook Account IDs, Instagram Account IDs and photographs.</p> <p>The plaintiffs have obtained an interlocutory injunction from the High Court against the defendants and any third parties who may be involved in the alleged unlawful disclosure of personal data. A breach of the terms of such interlocutory injunction may constitute a contempt of court.</p>	September 2019	<p>Hong Kong High Court Action Number 1741 of 2019</p> <p>(please approach our Hong Kong contacts for a copy of the writ)</p>

Malaysia

Contributors



Brian Law
Partner
T: ++65 6361 9873
brianlaw@
eversheds-harryelias.com



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

Development	Summary	Date	Links
Central Bank of Malaysia's policy document on 'Risk Management in Technology' (RMiT) applicable to financial institutions	<p>This policy document issued by Bank Negara Malaysia ("BNM") applicable to Financial Institutions ("FIs") such as licensed banks, licensed insurers, licensed takaful operators, prescribed development financial institutions, eligible issuers of e-money and operators of designated payment systems is intended to standardize the minimum compliance requirements on cybersecurity management employed.</p> <p>See our Spotlight on... briefing for more information.</p>	<p>Issued on: 18 July 2019</p> <p>Effective on: 1 January 2020</p>	<p>Bank Negara Malaysia Risk Management in Technology</p>
Scope of the Personal Data Protection Act ("PDPA") and planned amendments to be incorporated	<p>While the scope and function of the PDPA has been considered outdated for some time, this issue has been galvanized through headlines of a sordid political scandal. It has now been clarified through the Ministry of Communications and Multimedia Deputy that closed-circuit television (CCTV) recordings are subject to the PDPA and hotel management who operate such systems must be registered with the Data Protection Department under the Ministry to ensure its protection.</p> <p>Additionally, with the global impact of the EU's GDPR affecting multinational businesses in Malaysia, the Ministry of Communications and Multimedia has reverberated again that several major changes are expected, to better align Malaysia's Data Privacy laws to international standards. These changes are expected to focus on incorporating the additional requirements of the GDPR, focusing on cross-border data transfers through a white-list and mandatory breach notifications in light of the growing cyber-attacks committed this year.</p>	<p>CCTV Update: July 23 2019</p> <p>PDPA Review: ongoing since 2018</p>	<p>Personal Data Protection Act 2010 (Act 709)</p>
Inauguration of the 'Coordinated Malware Eradication and Remediation Platform' ("CMERP")	<p>After Cybersecurity Malaysia's partnership with Interpol in publishing the Global Guidelines for Digital Forensics Laboratories, the national agency turned to implementing a new platform in the prevention of cyberthreats - CMERP. This five-component automated detection managed by a coordinated intelligence system prevents and redirects malicious network traffic through a sinkhole that quarantines infected devices via a walled garden for subsequent</p>	<p>Launched on: September 23 2019</p>	<p>CMERP Website</p>



Development	Summary	Date	Links
	<p>removal. CMERP has been developed using local expertise through public-private collaboration is expected to significantly reduce the impact of malware threats for organisations, especially the Critical National Information Infrastructure ("CNII") sectors. First reactions to this announcement at the 11th Cyber Security Malaysia Awards, Conference and Exhibition Conference have been welcoming with high expectations.</p>		



Mauritius

Contributors



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



Jessimee Mootoosamy
Associate
T: +230 211 0550
jessimeemootoosamy@
eversheds-sutherland.mu

Development	Summary	Date	Links
The Mauritius Central Automated Switch ("MauCAS"), a novel state-of the art digital hub, launched by the Bank of Mauritius	<p>The MauCAS, which is fully owned and operated by the Bank of Mauritius for routing payments among operators on a 24/7 basis and the first national payment platform to operate round the clock, has been launched at the seat of the Bank of Mauritius.</p> <p>Built on open standards, the goal of MauCAS is to create an enabling environment for digital payments, which will support the development of Mauritius into a digital economy. MauCAS will therefore enable banks and non-bank operators to provide transformative payment and value-added services through cards, mobile phones and other innovative channels.</p>	Launched: 14 August 2019	MauCAS, the new electronic payment option
International Conference on the Next Generation Computing Applications ("NextComp") organised for the second time in Mauritius	The University of Mauritius organised its second International Conference on Next Generation Computing Applications, ("NextComp2019"). NextComp2019 is a major conference having a main goal of addressing new developments both in theory and in practice in the area of Communication and Computer Networks, Security and Forensics, Intelligent Systems, Data Analytics, Information Management, Bioinformatics and ICT Practices & Applications.	Conference held: 19-21 September 2019	NextComp 2019



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
New SARB Directive: reporting on material information technology and/or cyber incidents	<p>The South African prudential regulator, the Prudential Authority (the "PA"), issued a new directive on 10 September 2019 (the "Directive") under the Banks Act, which sets out the minimum reporting requirements that must be made by a bank to the PA in relation to 'material incidents' that are IT and/or cyber related.</p> <p>In its introduction to the Directive, the PA makes reference to the Bank for International Settlements' Financial Stability Institute's (FSI) paper, titled 'FSI Insight on policy implementation No 2: Regulatory Approaches to Enhance Bank's Cyber-Security Frameworks', which requires banks to establish a sound governance framework, with clear accountabilities with regard to cyber-risk, as IT specifically exposes banks to cyber-risk and cyberattacks.</p> <p>The Directive defines: (i) a 'material incident'; (ii) an 'IT incident'; (iii) a 'cyber incident'; and (iv) an 'information system'. Any bank must notify the PA as soon as practically possible, but not later than 1 day, after discovery of a material IT or cyber incident (which terms are broadly defined). After an incident has been reported to the PA, the bank will need to complete the 'Material IT and Cyber Incident Report' (Annexure A to the Directive), and submit a root cause and impact analysis report to the PA within 14 calendar days of the initial notification.</p> <p>In addition to these reporting obligations, the Directive requires banks to establish and maintain robust governance structures, which includes the coverage of IT, to ensure adequate management and operational oversight over critical business functions, resources, and infrastructure, and to implement a sufficiently robust incident management framework to manage and report IT and cyber incidents.</p>	Published: 10 September 2019	Executive summary Discussion paper



Contributors

United States



Michael Bahar
Partner

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



Alexander Sand
Associate

T: +1.512.721.2721
alexandersand@
eversheds-sutherland.com

In September, the California legislature passed five out of six pending bills to amend the California Consumer Privacy Act of 2018 ("CCPA"). At the time of publication, we expect the Governor to sign those bills – [AB-25](#), [AB-874](#), [AB-1146](#), [AB-1355](#) and [AB-1564](#)—into law on Friday 11 October 2019.

These amendments made significant changes to the law, the highlights of which are below:

- provide for a one-year exemption for HR and benefits data. However, this exemption does not apply to the privacy policy disclosure aspects of the CCPA, only the rights obligations. So, under § 1798.100(b) of the CCPA, a business would still need to, at or before the point of collection, inform the employees or contractors of "the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." In addition, starting on 1 January 2020 the business would not be able to "collect additional categories of personal information or use personal information collected for additional purposes" without first providing the consumer with a new notice. This one year exemption also does not apply to the Private Right of Action. Accordingly, under §1798.150, a business could be held liable if employee or contractor personal information is breached as "a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information";
- change the definition of "personal information" to subject to the requirements of the CCPA to information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household". The addition of a reasonableness qualification provides some relief from the strict construction of the existing language (Cal. Civ. Code § 1798.140(o)(1));
- further clarify that "personal information" does not include "consumer information that is de-identified or aggregate consumer information." (Cal Civ. Code § 1798.140(o)(3));
- the amendments also clarify and simplify the meaning of "publicly available information" to include all information lawfully made available from government records, without having to consider the purpose for which those records are made public or whether there are any conditions associated with the public records (Cal Civ. Code § 1798.140(o)(2)). Publicly available information is exempted from the definition of "personal information" and the requirements of the CCPA;
- clarify that the CCPA's deletion right shall not apply to the extent it is necessary to maintain the consumer's personal information to "fulfill the terms of a written warranty or product recall conducted in accordance with federal law" (Cal Civ. Code § 1798.105(d)(1));
- amend § 1798.145(i) so that it now reads: "This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or re-identify or otherwise link information that is not maintained in a manner that would be considered personal information." (Cal. Civ. Code 1798.145(i)). This may be particularly significant for the collection of Internet Protocol ("IP") addresses. The CCPA includes IP addresses within its definition of personal information, however, companies do not necessarily collect or retain IP address in a personally identifiable way, especially since most IP addresses are dynamic. This amendment could be read to clarify that the business would not have to go to an Internet Service Provider to find out which IP address was assigned to which user/household during what timeframe. This amendment is also significant in relation to verifying consumer requests. In fact,

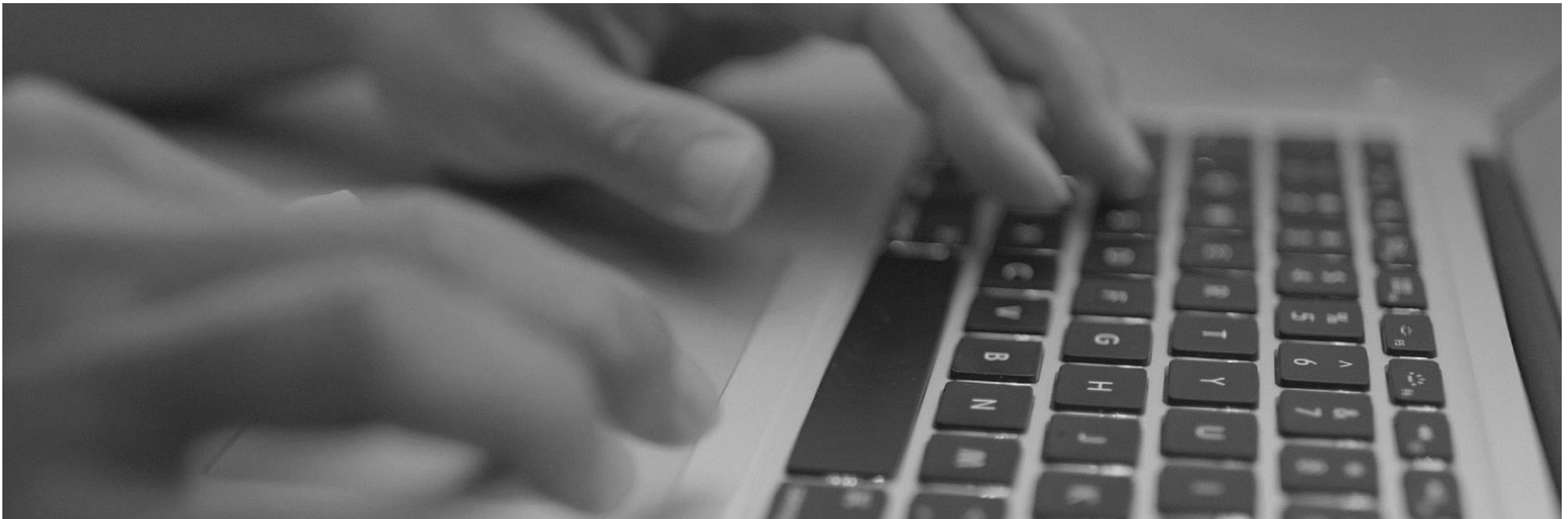


one amendment changes the definition of “verifiable consumer request,” to state that a business is “not obligated to provide information to the consumer pursuant to § 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.” (Cal Civ. Code § 1798.140(y));

- amend § 1798.150(a)(1) to clarify that class-action lawsuits may be brought for data breaches pursuant to California’s data breach notification law only when the personal information is “nonencrypted and nonredacted.” (Cal. Civ. Code § 1798.150(a)(1)); and
- clarify the extent of the § 1798.145(d)(1) exemption for personal information covered by the Fair Credit Reporting Act (“FCRA”), but does not exclude FCRA data from the private right of action.

The amendments also make revisions to the anti-discrimination right, clarify that a business only operating online needs to only provide an email address as a designated consumer request method, and provides for a one-year exemption from the CCPA for personal information exchanged as part of a Business-to-Business transaction (although similar to the one year exemption for HR data, the exemption does not apply for purposes of the Private Right of Action, nor does it exempt B2B customer data from the opt-out of sale right (Section 1798.120), but the opt-out of sale notice provisions in Section 1798.135 would not apply to businesses).

One notable bill that did not pass was [AB-846](#), which would have addressed the law’s application to customer loyalty programs.



Russian Federation

Contributors



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



Ekaterina Mironova
Senior Associate
T: +7 495 662 6434
ekaterina.mironova@
eversheds-sutherland.ru



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

Development	Summary	Date	Links
E-money in B2B business	<p>On 3 July 2019, the President of the Russian Federation signed into law a bill which introduces amendments to Federal Law No.161-FZ of 27 June 2019 'On the national payment system'.</p> <p>Starting in 2021, companies will be able to make payments to each other using 'electronic money'.</p> <p>For the purposes of this law, 'electronic money' are funds that are transferred using electronic means without the use of a bank account, through the use of a third-party proxy, to cover the payer's obligations to a payee who exclusively accepts electronic payment.</p> <p>Currently, B2B transfers of electronic money are prohibited. Companies and individual entrepreneurs can only make such transfers to individuals (and not to each other).</p>	<p>Effective: 1 January 2021 (these provisions)</p>	N/A
'Regulatory Sandbox' bill	<p>This bill was prepared by the Ministry of Economic Development. Legal entities developing digital technologies will have the opportunity to use experimental legal regimes – 'Regulatory Sandbox'. The intention is to reduce costs and the amount of time necessary to introduce innovative products, reduce legal risks, accelerate the launch of new solutions on the market, and filter out ineffective business models.</p> <p>The experimental legal regime will imply the application of special regulation for some time. This means that digital technology developers</p>	N/A	Bill text



Development	Summary	Date	Links
	<p>will not be subject to regulations that impede the implementation of innovations. Of course, there will be some exceptions to this rule, in particular, consumer protection legislation will still be applicable.</p> <p>It is worth noting that the Russian Central Bank has operated a similar experimental legal regime for financial products since 2018.</p>		
New data localization requirements for domestic flights and new requirements for automated systems within air transportation	<p>Recently, the Russian Government issued Government Decree No. 955, dated 24 July 2019.</p> <p>The Government Decree introduces requirements for automated information systems for the registration of air transportation (hereinafter “Automated Systems”), databases used in such information systems, the information and telecommunication networks related to such systems, their operators, the protection of information contained therein, and the details of their operation. This Government Decree has been adopted pursuant to the Air Code of the Russian Federation.</p> <p>Under the Government Decree, Automated Systems include in particular the following:</p> <ul style="list-style-type: none"> – reference information systems; – inventory reservation systems; – passenger and luggage registration systems; – automated distribution systems; and – settlement systems. <p>Operators of Automated Systems must ensure certain functionality and must meet certain requirements. The Government Decree also establishes a requirement that all operators of Automated Systems must be legal entities incorporated under Russian law.</p> <p>All databases and processing computer systems (servers) of the Automated Systems handling data related to domestic flights within Russia must be located on Russian territory. A domestic flight is defined as a flight for which the points of departure, destination and any stopovers are located on the territory of the Russian Federation.</p>	31 October 2021	N/A
Increase of liability for non-compliance with the	In June 2019 a bill was submitted to Russian Parliament to introduce administrative liability for non-compliance with the localization requirement	N/A	Bill text



Development	Summary	Date	Links
requirement of personal data localization bill	<p>of Russian data protection legislation (the “Bill”). The Bill recently passed its first reading in the Russian Parliament (Russian State Duma).</p> <p>Russian legislation does not currently provide for direct administrative liability in case of non-compliance with the localization requirement. Under current rules, it is nevertheless possible for the competent authorities to restrict access to a particular website in such cases.</p> <p>Under Russian data protection legislation, when a personal data operator collects personal data belonging to Russian citizens, including through the internet and information and telecommunication systems, the operator must record, systematize, accumulate, store, clarify, update, change and retrieve such personal data belonging to Russian citizens using a database located on the territory of the Russian Federation (the “Localization Requirement”), except for certain cases regulated in the law (for example, if data processing is directly required by Russian law).</p> <p>If the Bill is passed, operators of personal data may be brought to administrative liability for infringements of the legal obligations related to the Localization Requirement. The Bill envisages administrative fines of up to RUB 6,000,000 (approx. EUR 85,000) for companies and up to 500,000 (approx. EUR 7,000) for company officials; for repeated violations, these may go up to RUB 18,000,000 (approx. 250 000 euro) for companies and up to 1,000,000 (approx. EUR 14,000) for company officials.</p> <p>If passed, operators’ liability for the protection of personal data will see a significant increase in scope.</p>		



Spotlight on...

- EU: We look at the CJEU ruling in relation to the use of social media plugins and joint controllership
[Read more...](#)
- EU: We review the EDPB's draft guidelines for the use of video devices (including CCTV).
[Read more...](#)
- Germany: We examine Germany's new model for calculating fines for GDPR infringements.
[Read more...](#)
- Germany: We look at a recent decision from the High Regional Court of Frankfurt am Main in relation to the requirements for a valid consent.
[Read more...](#)
- US: We discuss the litigation risks under the CCPA
[Read more...](#)
- Ireland: We examine the Irish Data Protection Commissioner's new guidance on data sharing in the public sector.
[Read more...](#)
- UK: We consider the ICO's new guidance on "manifestly unfounded" and "excessive" in the context of responding to individuals' rights.
[Read more...](#)
- UK: ICO updates guidance on timescales for responding to individuals' rights: Date of receipt is 'day one'.
[Read more...](#)
- UK: We analyse the ICO's long awaited draft data sharing code of practice.
[Read more...](#)
- UK: We consider "Operational Resilience" and the key considerations for regulated financial institutions when outsourcing critical functions or activities.
[Read more...](#)
- Malaysia: We discuss the new technology risk policy document issued by the Central Bank of Malaysia.
[Read more...](#)

For further information, please contact:



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



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



@ESPrivacyLaw

eversheds-sutherland.com

© Eversheds Sutherland 2019. All rights reserved.

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

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

LON_LIB1\21369317\1

