EVERSHEDS SUTHERLAND

Commercial bulletin

May 2019

Welcome to the Eversheds Sutherland monthly commercial bulletin covering both case law and regulatory developments as well as progress on Brexit

Topics covered

Click on your topic of interest below:

- Brexit
- Commercial – general
- Consumer law
- Data protection, privacy and cyber-security
- IP
- IT
- Public sector

Brexit

Development	Summary	Links
New Withdrawal Agreement Bill awaited	On 21 May the Prime Minister gave a speech stating that a revised Withdrawal Agreement Bill, intended to break the current deadlock in Parliament and incorporating a "new Brexit deal", would be published this week. According to the speech of 21 May, the revised Withdrawal Agreement Bill will provide for the following: • the government will be placed under a legal obligation to conclude alternative arrangements to the Northern Ireland backstop by December 2020. If the backstop comes into force the government will ensure that Great Britain will stay aligned with Northern Ireland and will prohibit the proposal that a future government could split Northern Ireland off from the UK's customs territory • the House of Commons will approve the UK's objectives for the negotiations on the future UK-EU relationship and will approve the treaties governing that relationship before they are signed • the UK will seek as close to frictionless trade in goods with the EU as possible while outside the single market and ending free movement • the House of Commons will decide between the government's existing proposal for the future UK-EU customs arrangement and a compromise of a temporary customs union for goods, with the outcome of this decision to be reflected in legislation • a requirement for the House of Commons to vote on whether to hold a second referendum • a legal duty to secure changes to the political declaration to reflect this new deal However, publication of the revised Bill was postponed following the Prime Minister's announcement of her resignation, effective on 7 June, so it remains to be seen what its terms will be when published.	PM speech of 21 May
Government guidance on importing and exporting	The UK government has published step by step guidance on what businesses need to do to get ready to export from the UK to the EU, or to import from the EU to the UK, after Brexit. It has also published a country by country guide on exporting following a no deal Brexit.	Export guidance Import guidance Country by country guide to exporting on a no deal Brexit

Development	Summary	Links
UK progress on rolling over EU trade agreements	On 26 April the House of Commons Library published a briefing paper on UK progress in rolling over EU trade agreements that are expected to no longer apply to the UK either on a no deal Brexit or at the end of any transition period if there is a deal. The government also maintains a page on its website providing a list of the trade and mutual recognition agreements that the UK has signed with non-EU countries, as well as a page setting out the status of agreements and the implications if agreements are not in place in time for a no deal Brexit.	Briefing paper Signed UK trade agreements transitioned from the EU Existing trade agreements if the UK leaves the EU with no deal
No deal Brexit: SIs published in May	The no deal Brexit SIs published this month that are likely to be of interest to commercial practitioners include: The Electronic Communications (Amendment etc) (EU Exit) Regulations 2019 These Regulations amend legislation relating to the notification of personal data breaches by providers of publicly available electronic communications services and revoke direct EU legislation which is redundant or inappropriate after Brexit. The Trade Remedies (Reconsideration and Appeals) (EU Exit) Regulations 2019 These Regulations are made under the Taxation (Cross-border) Trade Act 2018 and set out the mechanism via which interested parties will be able to request reconsideration of and/or appeal against trade remedy decisions made by the Trade Remedies Authority and the Secretary of State. The Geo-Blocking Regulation (Revocation) (EU Exit) Regulations 2019 These Regulations revoke the retained EU law version of the Geo-Blocking Regulation 2018 as well as the Geo-Blocking Enforcement Regulations 2018. This legislation will be revoked on a no deal Brexit because of the loss of the reciprocity that is required in order for it to function effectively. The Consumer Rights Act 2015 (Enforcement) (Amendment) Order 2019 These Regulations enable the Secretary of State and the Office of Product Safety and Standards on his behalf (as well as enforcement authorities in the UK in respect of certain types of unsafe product) to investigate claims about unsafe consumer products that fall solely within the ambit of the General Product Safety Regulations 2005, through the use of the investigatory powers listed in Schedule 5 to the Consumer Rights 2015.	
Statutory guidance on sanctions	The Secretary of State for Foreign and Commonwealth Affairs has published statutory guidance under section 43 Sanctions and Anti-Money Laundering Act 2018 regarding the operation of the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 in the event of a no deal Brexit.	Statutory guidance

Commercial – general

Development	Summary	Links
Why you should always ensure that payment account details are set out in a contract	In K v A it was held that an obligation to make payment in cash to the seller's bank account meant payment to the seller's bank for the account of the seller. The buyer was therefore in breach of contract because it had made payment to a different account due to an email containing the correct account details being fraudulently intercepted and changed. This case highlights how important it is to include payment account details in the contract itself and to provide that these can only be changed via the contractual change control or variation procedure and not simply by the receiving party giving notice to the paying party.	Judgment
Advocate General Opinion that Airbnb is an information society service	An information society service ("ISS") is defined in the E-commerce Directive 2000/31 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". The purpose of the E-commerce Directive is to facilitate e-commerce across the EEA and remove barriers to trade. It establishes a "country of origin principle", a reciprocal arrangement whereby: • any EEA based ISS is only subject to the laws of the EEA state in which it is established where those laws relate to the "coordinated field" (ie laws relating to the activities of an ISS, such as qualifications or authorisations it needs to hold and its behaviour); and • the ISS benefits from the freedom to provide its services in all other EEA states without having to comply with each state's laws in the coordinated field (although there are some circumstances in which a state can derogate from this principle). Advocate General Szpunar has given an Opinion that the services provided by Airbnb Ireland (consisting of connecting, via an online platform, potential guests with hosts offering accommodation to rent) fall within the definition of an ISS. His reasoning is as follows: • The service is provided for remuneration and upon individual request, thereby fulfilling two of the criteria in the definition of an ISS. • In a situation where the services provided comprise an element that is provided by electronic means and an element that is not, the key issue is whether or not the material/physical service is inseparably linked to the service provided by electronic means. This requires two questions to be asked: o does the service provider offer services having a material/physical content?; and	Judgment

Development	Summary	Links
	o if so, does the service provider exercise decisive influence on the conditions under which such services are provided? If the services are not inseparably linked then it is possible for the service provided by electronic means to fall within the definition of an ISS. • Here, the accommodation service (ie the material/physical service) is not inseparably linked to the service provided by Airbnb by electronic means because: o the accommodation service can be, and often is, provided independently of the electronic service; and o Airbnb does not exercise control over how the accommodation service is provided, eg it exercises no control over location and standard of accommodation nor price. • This is in contrast to the Uber case in which it was found that the service provided by Uber of connecting non-professional drivers using their own vehicles with persons wishing to make urban journeys was not an ISS because the electronic service was inseparably linked to the transport service; but for the electronic service the transport service could not exist. • Airbnb also offers other optional services to property owners, such as photography, civil liability insurance and a guarantee for damage, but these services are also not inseparably linked to the service provided by electronic means and therefore are not capable of affecting the nature of that service If followed by the CJEU this Opinion will provide welcome clarification on how to assess whether new online service models driven by the gig economy fall within the scope of an ISS.	
Court of Appeal guidance on competing jurisdiction clauses	In a dispute over jurisdiction, the Court of Appeal has provided a useful summary of the approach the courts should take to the construction of jurisdiction clauses where the parties have entered into multiple, usually interdependent, contracts containing different jurisdiction clauses. • Where the parties' overall contractual arrangements contain two competing jurisdiction clauses, the starting point is that a jurisdiction clause in one contract was probably not intended to capture disputes more naturally seen as arising under a related contract. • The court should take a broad, purposive and commercially minded approach.	Judgment

Development	Summary	Links
	• Where the jurisdiction clauses are part of a series of agreements they should be interpreted in the light of the transaction as a whole. • Sensible business people are unlikely to intend that similar claims should be the subject of inconsistent jurisdiction clauses. • The starting presumption will therefore be that competing jurisdiction clauses are to be interpreted on the basis that each deals exclusively with its own subject matter and they are not overlapping, provided the language and surrounding circumstances so allow. • The language and surrounding circumstances may, however, make it clear that a dispute falls within the ambit of both clauses. In that event the result may be that either clause can apply rather than one clause to the exclusion of the other. This case demonstrates that when dealing with a suite of related contracts it is prudent to sense check the governing law and dispute resolution provisions in each contract against the others to ensure that it is clear how disputes that may relate to or impact on more than one contract will be dealt with.	
EU Directive to tackle unfair trading practices in agricultural and food supply chains	Directive 2019/633 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain has been published in the OJEU. This Directive seeks to eliminate unfair trading practices which arise due to significant imbalances in bargaining power between suppliers and buyers of agricultural and food products, by establishing a minimum list of prohibited unfair trading practices. Member States are required to adopt and publish implementing laws by 1 May 2021 and these will need to come into effect by 1 November 2021.	Directive
Summary of responses: cash and digital payment in the new economy	HM Treasury has published a summary of responses to its call for evidence into cash and digital payments in the new economy, which was issued to understand the trends impacting the way that payments are made. The document also includes the following key points: • the government is committed to supporting digital payments whilst safeguarding access to cash for those who need it; • HM Treasury will set up and chair a Joint Authorities Cash Strategy Group to facilitate coordination between authorities and provide comprehensive oversight of the overall cash infrastructure; • the government confirms it has no plans to alter the current make up of UK coins and notes in circulation; and	Summary of responses

Development	Summary	Links
	) the government notes that there is a perception that cash is sometimes used for tax evasion and money laundering and will consult on options to reduce these risks.	
Consultation on cryptoassets, DLT and smart contracts	The UK Jurisdiction Taskforce has launched a consultation to identify key issues of legal uncertainty regarding cryptoassets, distributed ledger technology (or blockchain) and smart contracts. The Taskforce is coordinating the preparation of an authoritative legal statement on the status of cryptoassets and smart contracts under English private law, with the intention that this will either demonstrate that English private law already provides sufficient certainty or highlight areas of uncertainty that need to be clarified. With regard to smart contracts, the proposed questions centre on enforceability with the principal question being "in what circumstances is a smart contract capable of giving rise to binding legal obligations enforceable in accordance with its terms?". This is then supplemented by a series of ancillary questions. The consultation also includes a useful explanation of the key features of its subject matter.	Link to consultation
Final report on independent review of the Modern Slavery Act 2015 published	The final report of the independent review into the Modern Slavery Act 2015, containing 80 recommendations, was laid in Parliament on 22 May. Of particular interest to businesses will be the recommendations relating to transparency in supply chains and the requirement for businesses over a certain size to publish an annual modern slavery statement (section 54 statement). These recommendations include that:) the government should establish an internal list of companies required to publish a section 54 statement ;) section 54(4)(b), which allows a company to say in its section 54 statement merely that it has taken no steps to address modern slavery in its supply chains, should be removed;) the six areas that a section 54 statement is currently recommended to cover should become mandatory;) the legislation should be amended to require companies to consider the entirety of their supply chains in respect of modern slavery;) there should be a central government repository to which section 54 statements have to be uploaded;) statutory guidance should be strengthened to include a template for a section 54 statement and to make it clear that reporting should not only include details	Final report

Development	Summary	Links
	of what businesses have done to prevent modern slavery in their supply chains but also the steps they intend to take in the future; • the Companies Act 2006 should be amended to include a requirement for companies to refer to their section 54 statement in their annual reports; • businesses should have a designated board member who is personally accountable for production of the section 54 statement and failures to fulfil reporting requirements or to act if an instance of slavery is found should be offences under the Company Directors Disqualification Act 1986; • the approach to tackling non-compliance with section 54 should be strengthened, including with the introduction of fines; • section 54 should be extended to the public sector; and • non-compliant companies should not be eligible for public contracts.	
Government response to Select Committee Scrutiny of Bribery Act 2010	In March this year the House of Lords Select Committee published its final report on its Post Legislative Scrutiny of the Bribery Act 2010. The government has now responded to the conclusions and recommendations of that report. Its response includes the following statements: • a number of measures have been introduced within the Specialist Fraud Division of the CPS to ensure that cases progress effectively and the SFO's Business Plan for 2019/20 outlines how the SFO will speed up fraud and bribery investigations; • the government notes that the MoJ guidance on the Bribery Act was drafted in a deliberately high-level, non-prescriptive way: there are other organisations that could provide sector specific guidance on what is and isn't acceptable corporate hospitality and the guidance will not be amended to provide more examples of what might provide a good defence to the offence of failing to prevent bribery by associated persons; and • the Director of the SFO will shortly publish guidance for corporates who wish to self-report.	Government response
Government response to report on disinformation and fake news	The government has published its response to the Digital, Culture, Media and Sport Committee report on disinformation and fake news (published in February). The response notes that many of the report's recommendations are in line with and addressed in the White Paper on Online Harms published in April and contains many cross-references to this White Paper. Amongst other things, the response also:	Government response

Development	Summary	Links
	• rejects the creation of a new category of tech company which is neither a platform nor a publisher and which is liable for harmful content posted by users; instead the government favours a statutory duty of care and codes of practice enforced by an independent regulator with powers to take action against breaches, including the ability to levy substantial fines; • agrees that social media companies have not provided sufficient access to data to allow for the collection of robust information and states that a key objective of the new regulatory framework will be to develop a culture of transparency, trust and accountability which will include information gathering powers for the regulator; and • notes that the recommendations contained in the report of the Digital Competition Expert Panel that was published in March (the "Furman Review") fit with the government's strategy for an open and competitive economy.	

Consumer law

Development	Summary	Links
Consultation on proposals to regulate consumer IoT device security	In October 2018 the government published a voluntary Code of Practice for Consumer IoT Security which is intended to support all stakeholders involved in development, manufacturing and sale of consumer IoT devices. However, the government is concerned that despite the introduction of this Code of Practice there are still significant security flaws in many products on the market and this situation needs to be addressed urgently in order to protect both consumers and the wider economy. It therefore intends to introduce legislation to regulate this area and to ensure that all consumer IoT devices meet basic security standards. On 1 May it launched a consultation on its regulatory proposals, including the introduction of a new mandatory security labelling scheme for consumer IoT products to assist consumers in making informed purchasing decisions. The consultation closes on 5 June 2019. Click on the link to read our briefing on this topic.	Eversheds Sutherland briefing Consultation
New consumer protection Directives published in OJEU	On 22 May two new Directives which form part of the European Commission's Digital Single Market Strategy, Directive 2019/770 on digital content and digital services and Directive 2019/771 on certain aspects of contracts for the sale of goods, were published in the OJEU. The digital content Directive introduces increased protection for consumers paying for a service and also for those providing data in exchange for a service. For example, the new rules provide that if it is not possible to fix defects within a reasonable amount of time, the consumer is entitled to a price reduction or full reimbursement. In addition, the guarantee period cannot be shorter than two years. The sales of goods Directive will apply to all goods, including those with a digital element (eg smart fridges). Here the new rules introduce a two year minimum guarantee period (from the time the consumer receives the good) and a one year period for the reversed burden of proof in favour of the consumer. Individual member states can go beyond those times to maintain their current level of consumer protection. The Directives enter into force on the 20th day following publication and Member States then have until 1 July 2021 to adopt and publish domestic implementing legislation, with such legislation to apply from 1 January 2022.	Digital content and digital services Directive Sale of goods Directive

Data protection, privacy and cyber-security

Development	Summary	Links
New sanctions for cyber-attacks which constitute an external threat to the EU	On 17 May Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States came into force. This establishes a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks (or attempted attacks) that have a significant impact and which constitute an external threat to the EU or its Member States. It allows the EU to impose sanctions on persons and entities that are responsible for such cyber-attacks or who provide support for them or are otherwise involved. Sanctions include travel bans and asset freezes. In the UK The Cyber-Attacks (Asset-Freezing) Regulations 2019 (SI 2019/956) have been laid before Parliament and will enter into force on 11 June 2019. The Regulations put in place the UK's domestic enforcement regime for the new sanctions regime set out in the Regulation.	EU Regulation The Cyber-Attacks (Asset-Freezing) Regulations 2019
NCSC guidance on cyber security design principles	The National Cyber Security Centre has published guidance setting out cyber security design principles which are intended to help ensure that networks and technologies are designed and built securely. The principles are divided into five categories which are loosely aligned with the stages at which an attack can be mitigated, namely, establishing the context (determining all the elements of the system so that there are no blind spots); making compromise or penetration difficult; making disruption difficult; making compromise detection easier; and reducing the impact of compromise.	Guidance
ENISA increases efforts to encourage cybersecurity with "Industry 4.0 Cybersecurity: Challenges and Recommendations" paper	ENISA (the EU's Agency for Cybersecurity) has published a new paper 'Challenges and Recommendations for Industry 4.0 Cybersecurity' which provides the results of a gap analysis conducted in order to identify the main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT. The report follows and builds on the recently published study on 'Good Practices for Security of IoT in the context of Smart Manufacturing'. In the report, ENISA lists high-level recommendations to different stakeholder groups in order to promote Industry 4.0 cybersecurity and facilitate wider take-up of relevant innovations in a secure manner. The key recommendations for stakeholders are: • promote cross-functional knowledge on IT & IoT security; • clarify liability amongst industry 4.0 actors; • foster economic and administrative incentives for industry 4.0 security; • harmonise efforts on industry 4.0 security standards; • secure supply chain management processes;	Press release Report

Development	Summary	Links
	) establish industry 4.0 baseline for security interoperability; and) apply technical measures to ensure industry 4.0 security.	
Government hosts roundtable on improving cybersecurity and Internet of Things devices	On 30 April, DCMS, the National Cybersecurity Centre (NCSC) and consumer group Which? met with representatives from IoT manufacturers and retailers to discuss the cyber security of consumer smart products. The meeting was chaired by Margot James MP, Minister for Digital and the Creative Industries and the purpose was for DCMS to understand the steps manufacturers are taking to secure their products and drive the adoption of security good practice.	News release
Call for evidence on online targeting and bias in algorithmic decision making	The Centre for Data Ethics and Innovation has issued calls for evidence on online targeting (defined as the customisation of products and services online based on data about individual users) and bias in algorithmic decision making. Responses are due by 14 June 2019.	Calls for evidence
European Data Protection Board guidance on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services	The European Data Protection Board (EDPB) has published a set of draft guidelines for public consultation on what "necessity" means for GDPR and tightening up "contract" as a lawful processing ground in the context of "online services". The guidelines are key to providers of online services, such as social media, e-commerce, internet search engines, communication and travel services. They also, by extrapolation, provide insight to other businesses on just how narrowly the application of this lawful basis is likely to be applied in other contexts. For further analysis, please read our briefing.	Draft guidelines and consultation details Eversheds Sutherland briefing Eversheds Sutherland eight point summary
French action against US Privacy Shield	In October 2016, La Quadrature du Net (a French non-profit association that defends the rights and freedom of citizens on the internet) brought an action calling for the US Privacy Shield framework to be annulled, alleging that the Privacy Shield infringes the Charter of Fundamental Rights of the European Union in particular due to the mass surveillance permitted under the US regulatory regime. The European Court of Justice is now set to hear the case on 1-2 July 2019. This is the latest development in a series of criticisms made against the Privacy Shield framework. By way of background, in June 2018 the European Parliament called for the European Commission to suspend the Privacy Shield if specific requirements were not implemented by 1 September 2018. However in December 2018, the European Commission published the findings of its second annual review of the EU-US Privacy Shield – finding that the US continued to ensure an adequate level of protection for personal data under the Privacy Shield. The Commission urged the US government to identify a nominee to fill the Ombudsperson position on a permanent basis by 28	La Quadrature du Net website post European Commission report (December 2019) EDPB report (January 2019) European Parliament statement (June 2018)

Development	Summary	Links
	February 2019 otherwise, the Commission would consider taking "appropriate measures," in accordance with GDPR. More recently in January 2019, the EDPB adopted a report on the Second Annual Review of the EU-US Privacy Shield. The report noted the concerns already expressed by the EDPB's predecessor, the Article 29 Working Party, on the lack of concrete assurances that indiscriminate collection and access of personal data for national security purposes are excluded. In addition, the EDPB noted that the Ombudsperson is not vested with sufficient powers to remedy non-compliance, and that checks regarding compliance with the substance of the Privacy Shield's principles are not sufficiently strong. The EDPB also highlighted additional concerns in relation to checks to comply with the onward transfer requirements, the scope of meaning of HR Data and the recertification process, and a list of remaining issues raised after the first joint review which are still pending. Organisations relying on the US Privacy Shield framework to legitimise transfers of personal data should continue to monitor developments.	
ICO compels HMRC to delete unlawfully collected voice data	On 4 April 2019, the ICO issued a preliminary enforcement notice compelling HMRC to delete all biometric data collected under HMRC's Voice ID system for which it does not have explicit consent before 5 June 2019. The ICO investigated HMRC's Voice ID service after receiving a complaint from Big Brother Watch, a non-profit non-party British civil liberties and privacy campaigning organisation, regarding the department's practices. The ICO examined HMRC's use of voice recognition and authentication software for verification purposes since January 2017, and found that HMRC did not give individuals sufficient information about how their biometric data would be processed. In addition, HMRC did not obtain individuals' consent or provide them with the means of withholding consent. It was also found that HMRC did not complete a data protection impact assessment before launching the system. HMRC have agreed to delete all records for which they do not hold explicit consent – approximately 5 million customers – but will continue to use the Voice ID system, confirming that changes were introduced in October 2018 to ensure the system's compliance with GDPR requirements. The ICO plan to follow up the investigation with an audit to assess HMRC's compliance with good practice in the processing of personal data. Organisations planning to use new technologies involving the use of personal data (including biometric data) should consider the key points emphasised in the ICO's blog post "Using biometric data in a fair, transparent and accountable manner".	ICO blog post ICO statement HMRC letter to DPO
Government forms Artificial Intelligence Council	The Government has established an independent expert committee to further the development of artificial intelligence across the UK, and promote its ethical use. The	Press release

Development	Summary	Links
	committee has been named the AI Council, and is made up of leaders from business, academia and data privacy organisations.	
ICO explores accuracy of AI systems and performance measures in latest blog posts	In the latest post from their AI auditing framework blog series, the ICO's AI specialist team considers how the data protection principle of accuracy may be applied to AI systems, and propose certain steps organisations should take to ensure compliance. In particular, the blog post explains why accuracy is important for the outputs of AI systems, in respect of the accuracy of decisions or predictions about a specific person and across a wider population. The post also examines accuracy as a performance measure. The ICO recommends that where organisations decide to adopt an AI system, they should: • ensure that all functions and individuals responsible for its development, testing, validation, deployment, and monitoring are adequately trained to understand the associated accuracy requirements and measures; and • adopt an official common terminology that staff can use to discuss accuracy performance measures, including their limitations and any adverse impact on data subjects. In a later post, the team examines how AI can exacerbate known security risks and make them more difficult to manage. The team notes that in ICO guidance the ICO recommends that organisations developing machine learning systems can further mitigate security risks associated with third party code, by separating the machine learning development environment from the rest of their IT infrastructure where possible, by deploying the following techniques: • use 'virtual machines' or 'containers' - emulations of a computer system that run inside, but isolated from the rest of the IT system. These can be pre-configured specifically for machine learning tasks; and • where appropriate, train the machine learning model using one programming language (eg Python) and then, before deployment, convert the model into another language (eg Java) that makes making insecure coding less likely.	ICO accuracy and AI blog post ICO security and AI blog post
ICO emphasises importance of paying data protection fee by drawing on recent enforcement action	In a recent blog post, the ICO's Deputy Chief Executive Officer discussed the importance of paying the data protection fee, drawing on recent ICO enforcement action. The First Tier Tribunal (Information Rights) dismissed an appeal by Farrow & Ball against a £4,000 penalty notice from the ICO for failure to pay the tier 3 data protection fee of £2,900. Farrow & Ball had appealed, citing that the failure to pay the fee was a mistake and that the ICO's reminder to pay was sent while the person responsible was on	ICO blog post Information Rights Tribunal decision

Development	Summary	Links
	holiday, the correspondence was not identified as important internally and the fee was paid promptly once the oversight was discovered.	
ICO calls for views on a data protection and journalism code of practice	On 29 April 2019 the ICO called for views on a data protection and journalism code of practice. The ICO have stated that they will use our existing media guidance as a framework to inform the code and will update the contents to reflect the requirements of the Data Protection Act 2018, and take account of developments in case law and the field of journalism more generally. The aim is to provide journalists and media organisations with a helpful, practical toolkit to assist them in complying with their data protection obligations. The ICO will work with other regulatory bodies which police standards in the journalism industry, such as IPSO, IMPRESS and Ofcom, to ensure the code fits within the wider framework.	ICO statement
Sharing of personal data of young persons	In R (on the application of M) v Chief Constable of Sussex [2019] EWHC 975 (Admin), the High Court found that it was appropriate to share certain data pertaining to a sixteen year old girl by way of an information sharing agreement between the police and a local business crime reduction partnership and this did not breach data protection laws. However, the sharing of the information that revealed the girl's vulnerability to child sexual exploitation breached her statutory data protection rights.	Judgment
ICO launches campaign to help people be data aware	Businesses should be aware that the ICO has launched a new campaign: "Be Data Aware", which aims to help people understand how organisations might be using their data to target them online (including to reach them with social media adverts to market goods or services and for political marketing), and how people can control who is targeting them (such as by using social media privacy settings). The campaign follows the ICO's ongoing investigation into the use of data analytics for political purposes, which recommended the continuation of education of the public on the use of data analytics in political campaigns and on the impact of new and developing technologies.	ICO statement
ICO seeks views from organisations considering certifications schemes and codes of conduct	In its May newsletter, the ICO has called for organisations to get in touch if they are considering developing a certification scheme (under Article 42 GDPR) and/or creating a sector specific code of conduct (under Article 40 GDPR). Certification is a way for organisations to demonstrate compliance with the GDPR. It can cover specific issues or be more general. The ICO has also updated its guidance on certification schemes. Trade associations and representative bodies may draw up codes of conduct covering topics important to their members to provide sector specific guidance about data protection law.	ICO newsletter (May 2019)

Development	Summary	Links
Digital Copyright Directive published in OJEU	Directive 2019/790 on copyright and related rights in the Digital Single Market (the Digital Copyright Directive) was published in the OJEU on 17 May. It will enter into force on 6 June 2019 and member states are required to bring implementing legislation into force by 7 June 2021. For more information on the content of the Digital Copyright Directive see our April commercial bulletin.	Directive
IPO guidance on implementation of the Marrakesh Directive	The IPO has published guidance on changes to UK copyright law to implement the Marrakesh Directive. This aims to improve access to copyright works by visually-impaired and print-disabled people, by making exceptions to copyright laws allowing accessible copies of copyright works to be made and transferred across borders.	Guidance
New service to tackle cybersquatting and bad faith domain name registrations	On 18 May a new service was launched by the EU IPO and EURid (the registry manager of the .eu and .ею country code top-level domains), which is aimed to help EU trade mark applicants tackle cybersquatting and bad faith domain name registrations. The service allows rights holders and applicants to opt-in to receive alerts as soon as a .eu or .ею domain name identical to their EU trade mark application is registered.	EUIPO press release EURid press release

Development	Summary	Links
EU Commission proposal for WTO legal framework on e-commerce	In January WTO members agreed to start negotiations for the agreement of a multilateral legal framework for the trade-related aspects of e-commerce. The EU Commission has now published a Communication setting out its proposals for this framework, which will be discussed alongside proposals by other members at WTO meetings this month. The EU's proposals include: • ensuring that e-contracts and e-signatures are valid • protecting consumers from fraudulent and deceptive commercial practices when they engage in e-commerce transactions and enhancing online consumer trust • protecting consumers against unsolicited commercial e-messages • ensuring cross-border data flows to facilitate trade in the digital economy, whilst ensuring the protection of personal data and privacy • banning customs duties on electronic transmissions • maintaining open internet access • upgrading existing WTO disciplines on telecoms services • improving market access commitments in telecoms and computer-related services	EU Commission Communication
OECD principles on AI	On 22 May 42 countries signed up to the Organisation for Economic Co-operation and Development (OECD)'s Recommendation on AI. The OECD states that this is the first set of intergovernmental policy guidelines on AI. The Recommendation sets out five values-based principles for the responsible deployment of trustworthy AI, namely: • AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being • AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards to ensure a fair and just society • there should be transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes	Principles

Development	Summary	Links
	• AI systems must function in a robust, secure and safe way throughout their lifetimes and potential risks should be continually assessed and managed • those developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles and five recommendations to governments: • facilitate public and private investment in research and development to spur innovation in trustworthy AI • foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge • create a policy environment that will open the way to deployment of trustworthy AI systems • equip people with the skills for AI and support workers to ensure a fair transition co-operate across borders and sectors to share information, develop standards and work towards responsible stewardship of AI	

Development	Summary	Links
House of Lords Constitution Committee report on Parliamentary scrutiny of treaties	The House of Lords Constitution Committee has published a report calling for reform of Parliamentary scrutiny of treaties, prompted by the need for the government to enter into an increased number of treaties, including complex trade treaties, as a result of Brexit. At present Parliament has no involvement in a treaty until it is signed, at which point there is a period of 21 Parliamentary sitting days in which the treaty can be scrutinised but with no guarantee that a debate or vote on ratification will actually take place during this period. The key recommendations of that report include: • the establishment of a new treaty scrutiny committee to sift all treaties, with power to scrutinise (or refer to other select committees for scrutiny) and recommend debates on significant treaties; • Parliament should be informed when negotiations begin and should be provided with better information about agreed treaties, with a general principle of transparency and disclosure of information to Parliament; and • the government should work closely with the devolved institutions during the treaty-making process.	Press release
Procurement Policy Note on e-invoicing	The Cabinet Office has published procurement policy note 03/19 on The Public Procurement (Electronic Invoices etc.) Regulations 2019. This contains a model clause which reflects the new requirement for contracting authorities and entities to include an express contract term obliging them to accept and process undisputed invoices that comply with the technical e-invoicing standard developed under the Directive implemented by the UK Regulations.	Procurement Policy note 03/19

For further information, please contact:

Sara Ellis
Principal Associate PSL

T: +44 121 232 1062
M: +44 7827 954 720
saraellis@eversheds-sutherland.com

Claire Stewart
Principal Associate PSL

T: +44 20 7919 4856
M: +44 7867 155 050
clairestewart@eversheds-sutherland.com

Lizzie Charlton
Senior Associate PSL (Data Protection & Privacy)

T: +44 20 7919 0826
M: +44 7827 230 131
lizziecharlton@eversheds-sutherland.com

eversheds-sutherland.com

BIR_COMM\1712598\1