e-Commerce 2020

Contributing editor
Robert Bond

LEXOLOGY®
Getting The Deal Through

© Law Business Research 2019

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and July 2019. Be advised that this is a developing area.

© Law Business Research Ltd 2019
No photocopying without a CLA licence.
First published 2000
Sixteenth edition
ISBN 978-1-83862-138-4

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

e-Commerce
2020

Contributing editor
Robert Bond
Bristows LLP

Getting the Deal Through is delighted to publish the sixteenth edition of e-Commerce, which is available in print, as an e-book, and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Croatia.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editor, Robert Bond of Bristows LLP for his continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

© Law Business Research 2019

Contents

© Law Business Research 2019

United Kingdom

Robert Bond
Bristows LLP

LEGAL AND REGULATORY FRAMEWORK

Government approach

1 | How can the government's attitude and approach to internet issues best be described?

The UK government's attitude to the internet could generally be described as favourable, with the government recognising that the digital sector is one of the UK's most important sectors; not just in terms of economic value but also because of its potential to promote growth and innovation. Against the backdrop of preparations to leave the European Union following the Brexit vote in 2016, the government has continued to develop policy and prepare legislation that acknowledges the benefit of an open, innovative and thriving digital sector for the United Kingdom.

In March 2017, the government published its policy paper on the UK's digital strategy, which forms part of the government's industrial strategy for the post-Brexit era. The purpose of the strategy paper is to encourage further investment into the UK's digital sector to help the country consolidate its position as a global hub for digital technology. Among other things, the strategy sets out the government's policy on digital infrastructure, skills and education, promoting digital business and internet security. Furthermore, in April 2017, the Digital Economy Act 2017 received royal assent. This legislation introduces a wide range of measures, such as those relating to powers for the UK regulator to introduce a statutory code to govern:

- direct marketing practices;
- measures relating to data sharing in the public sector;
- age-verification requirements for online pornography; and
- legal rights for individuals to request access to broadband and telecoms services.

Since the Brexit referendum in 2016, the UK government has continued to accept that new EU regulations are enforceable as law in the United Kingdom and has implemented EU directives by means of national legislation. This has extended to the field of e-commerce where the General Data Protection Regulation (GDPR) became applicable on 25 May 2018 and the UK's regulatory body, the Information Commissioner's Office (ICO) has taken an active role in issuing GDPR guidance and enforcing the powers granted to data protection authorities under the GDPR. In relation to cyber and network security, the UK government has implemented the Network and Information Security Directive (NISD) (see questions 2 and 35), with the National Cyber Security Centre providing support and guidance on compliance with its provisions. The United Kingdom also implemented the EU's Geo-blocking Regulation by way of Geo-blocking Enforcement Regulations 2018, which came into force on 3 December 2018. Now applicable to UK businesses, the EU's Geo-blocking Regulation prohibits discrimination against consumers and businesses on the basis of nationality, place of residence or establishment. Along with the regulations on cross-border portability of online content and parcel delivery services (see question 2), the Geo-blocking Regulation forms the basis of the EU Commission's digital single market strategy.

The UK government has indicated that once the United Kingdom is no longer subject to EU laws it will distance itself from the digital single market strategy. The ultimate fate of such EU-derived legislation is therefore uncertain and it is also unclear whether the United Kingdom will implement future directives, such as the Supply of Digital Content Directive and the Sale of Goods Directive, which the EU Parliament is due to approve in 2019. However, the UK government has recently advised online businesses and service providers that should the United Kingdom exit the European Union without a deal, it will seek to prioritise 'continuity and stability', aligning itself with the approach in the EU's E-Commerce Directive. The UK government's guidance, dated January 2018, on how online businesses and service providers should operate in the European Economic Area in the event of a no-deal Brexit, covers activities governed by the EU's E-Commerce Directive, including:

- online retail;
- social media;
- search engines;
- video-sharing sites; and
- internet service providers.

Legislation

2 | What legislation governs business on the internet?

There is a large amount of e-commerce-related legislation (which is based on EU legislation), including:

- the Consumer Rights Act 2015 (CRA), which came into effect in the United Kingdom on 1 October 2015 and is the biggest shake-up of consumer law in a generation. The CRA affects all businesses whether they are providing goods or services and whether those are tangible or intangible. The CRA also introduces consumer law relating to digital content for the first time;
- the GDPR governs the processing of all personal data such as customer names, addresses, payment details, etc and represents the largest overhaul in EU data privacy laws in more than 20 years, introducing new obligations on both data controllers and data processors and raising the maximum penalties for breaches to up to 4 per cent of worldwide turnover or €20 million, whichever is higher. The Data Protection Act 2018 (DPA 2018) replaces the Data Protection Act 1998 and supplements the GDPR, extending data protection laws to areas not covered by the GDPR;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003, which govern the use of cookies, location data, opt-in rules for marketing calls and email marketing, unsolicited marketing, etc;
- the Network and Information Systems Regulations 2018 (NIS Regulations) (as amended), implementing NISD, which require digital service providers, being organisations providing online

© Law Business Research 2019

marketplaces, online search engines and/or cloud computing services, to implement appropriate cybersecurity measures and report any incidents having a substantial impact on the provision of digital services;
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013, which require traders to provide information to consumers in relation to contracts concluded between them;
- Regulation (EU) 2018/644 on cross-border parcel delivery services, which sets out a transparency regime for cross-border parcel delivery service tariffs and requires traders to provide information on cross-border delivery options and complaints handling procedures to the consumer;
- Regulation (EU) 2017/1128 on cross-border portability of online content services in the internal market (Portability Regulation), supplemented by the Portability of Online Content Services Regulations 2018 (SI 2018/249), which requires online service providers of paid-for content to allow subscribers to portable online content services to access and use those services when temporarily present in another member state, without any additional charge;
- Regulation (EU) No. 2018/302 on geo-blocking, which prohibits discrimination against consumers and, in limited cases, against businesses, based on their nationality, place of residence or establishment when they buy goods or services. This was implemented by the Geo-blocking (Enforcement) Regulations 2018 (SI 2018/1153).
- the Consumer Rights (Payment Surcharges) Regulations 2012 (SI 2012/3110), as amended by the Payment Services Regulations 2017, which ban surcharges on the basis of a consumer's choice of payment instrument (eg, credit card, debit card or e-money);
- the Financial Services (Distance Marketing) Regulations 2004, which set out the rules on the information that must be supplied to consumers when financial services are sold at a distance;
- the Electronic Commerce (EC Directive) Regulations 2002 (as amended), which, among other things, dictate the information that consumers must be provided with in online transactions;
- the Consumer Protection from Unfair Trading Regulations 2008, as amended by the Consumer Protection (Amendment) Regulations 2014 (SI 2014/870), which regulate online advertising and govern the content of commercial communications or promotions to consumers, including comparative advertising, while the Business Protection from Misleading Marketing Regulations 2008 also regulate online advertising and govern the content of commercial communications or promotions to businesses. In respect of both of these regulations, the regulator takes the view that all required information must be shown together in one place so that it is capable of being read by the consumer as a whole. There are no specific rules or exemptions for internet advertising or other forms of electronic communication;
- the Consumer Protection Co-operation Regulation 2006, which grants national consumer protection authorities in the European Union greater powers to protect consumers against cross-border breaches of consumer protection laws;
- the Provision of Services Regulations 2009, which set out mandatory disclosure requirements and freedom of establishment for providers from another EU member state;
- the Alternative Dispute Resolution for Consumer Disputes (Competent Authorities and Information) Regulations 2015 (as amended), which establish a framework for accredited alternative dispute resolution (ADR) entities dealing with small consumer claims and information that traders have to provide to consumers about access to ADR;
- the Committee of Advertising Practise (CAP) and Broadcast Committee of Advertising Practice (BCAP) codes of practice applies to advertising;
- financial services legislation that applies to the provision of financial products and services; and
- criminal and defamation laws that apply to activities on the internet.

As noted in question 1, the European Union currently has additional proposals in the legislative calendar that are of relevance to online businesses:
- the Supply of Digital Content Directive; and
- the Sale of Goods Directive.

Currently, the ultimate fate of EU-derived legislation is uncertain. If the United Kingdom and the European Union conclude a withdrawal agreement before the United Kingdom exits the European Union, there will be a transition period during which most EU law will continue to apply to the United Kingdom. During the transition period, the United Kingdom will need to continue implementing EU law that falls within the scope of the withdrawal agreement. In these circumstances, the United Kingdom intends, by way of the withdrawal agreement and other statutory instruments, to transpose most EU law (albeit in a revised form, where appropriate) into domestic law. If the United Kingdom exits the European Union without a deal, there will be no transition period; EU law will no longer apply under the European Communities Act 1972 and the United Kingdom will no longer be obliged to implement EU law in domestic law.

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

No regulatory body has overall responsibility for the regulation of e-commerce as such, although a number of such bodies have interests in ensuring the enforcement of certain laws that apply to e-commerce (eg, the Chartered Trading Standards Institute is as concerned with protecting consumers against online rogue traders as it is with offline traders).

The Office of Communications (Ofcom) is the regulatory body responsible for ensuring competitive behaviour relating to access tariffs and charges. Ofcom's responsibilities are set out in the Communications Act 2003 and Ofcom also has powers under the Competition Act 1998, the Enterprise Act 2002 and under EU competition law to deal with anti-competitive behaviour. Pursuant to a market review by Ofcom in 2005, BT gave a number of undertakings relating to the price of wholesale broadband services.

Ofcom's powers were significantly increased by the Digital Rights Act 2010, which amended the Communications Act 2003. Ofcom has the right to limit or cut off internet access of a subscriber who has habitually infringed copyright, with the download of films or music illegally.

The Information Commissioner's Office (ICO) is the regulatory body associated with data protection. In relation to online activity, the remit of the ICO includes the monitoring of unsolicited marketing material by electronic mail (this includes texts, picture messages and emails), which should only be sent if the person has chosen to receive them, unless the email address was obtained as a result of a commercial relationship. The individual should always be given the opportunity to stop receiving the emails. The GDPR has extended the ICO's ability to carry out dawn raids against data controllers and processors. The ICO requires a warrant to enter premises, but with a valid warrant it can inspect and seize documents and materials found on the premises to determine whether data protection legislation has been complied with. Further to

© Law Business Research 2019

the implementation of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, the ICO's remit also includes ensuring that web hosts now obtain consent from users before using cookies and taking enforcement action when web hosts are in breach (see question 34).

The Advertising Standards Authority (ASA) is the UK's independent regulator of advertising across all media. The United Kingdom applies the CAP and BCAP advertising codes, which are written by the Committees of Advertising Practice. Sector-specific bodies such as the Financial Conduct Authority (FCA) oversee the marketing of financial products online.

Jurisdiction

4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

Issues of jurisdiction for internet-based transactions are governed by existing rules of private international law embodied with regard to disputes between EU consumers and businesses within the Convention on the Law Applicable to Contractual Obligations 1980 (Rome Convention) and Brussels Regulation 2000, incorporated into UK law by the Contracts (Applicable Law) Act 1990 and the Civil Jurisdiction and Judgments Order 2001 respectively.

In the context of consumer issues involving sellers located within the European Union, the broad intention is that EU consumers that purchase products from a business in another EU country that has been marketing its products to them should be entitled to the mandatory protections of their own country's consumer laws and have the dispute heard before the courts of their own country, regardless of what the business might state in its terms and conditions. The rules are, however, complex and what law applies and where a claim can be brought will depend on the facts of each case.

With regard to disputes that involve sellers that are not located within the European Union, the general position is that the contract will be governed by the law provided in the terms and conditions. The Rome Convention applies to contractual obligations where a choice of law is involved, even in some cases where the law it designates is that of a non-contracting state. The signatories to a contract may choose the law applicable to the whole or a part of the contract, and select the court that will have jurisdiction over disputes. By mutual agreement they may change the law applicable to the contract at any time (principle of freedom of choice).

Regulation (EC) No. 864/2007 on the Law Applicable to Non-Contractual Obligations (Rome II) was enacted in January 2009. It applies to non-contractual obligations arising in civil and commercial matters. The general rule is that the law applicable to non-

contractual obligations is the law of the country in which the damage occurs or is likely to occur. At the time of completing this note, nothing has been finalised with respect to Brexit; the ultimate position on jurisdiction for online businesses operating in the United Kingdom and the European Union is therefore uncertain.

In the event that the United Kingdom exits the European Union without a deal, the UK government has advised online businesses and service providers that it will seek to prioritise 'continuity and stability', aligning itself with the approach in the EU's E-Commerce Directive. Regardless of the UK's approach, UK-domiciled online service providers will no longer be able to take advantage of the 'country of origin principle' when operating in the European Economic Area. (The country of origin principle is a reciprocal arrangement that establishes that any EEA-based online business does not have to adhere to rules governing online activities in each EEA state in which they operate but instead should only be subject to certain laws in the state in which it is established.) In the event of a no-deal Brexit, online service providers will need to comply with the national laws governing online activities of each EEA member state. If the United Kingdom exits the European Union without a deal, entities making business-to-business sales in the European Economic Area must comply with the local laws of the EEA states in which the sales are made; this will mirror the position for those making business-to-consumer sales. EEA-based businesses will also be brought within the scope of UK law. The UK government, under the draft Civil Jurisdiction and Judgments (Amendment) (EU Exit) Regulations 2019, has indicated that it will also continue to enforce judgments given in other EU/EEA states where proceedings were initiated before the withdrawal date.

On 18 January 2019, the EU Commission published a notice titled 'Withdrawal of the United Kingdom and EU Rules In the Field of Civil Justice and Private International Law', which outlines the impact a no-deal Brexit will have on jurisdiction and the enforcement and recognition of UK judgments in EU member states. If the United Kingdom exits the European Union without a deal, the rules on international jurisdiction in EU instruments in the area of civil and commercial law will no longer apply to UK domiciled defendants (unless the EU law is applicable to third countries). International jurisdiction will be governed by the national rules of the member state in which a court is seized. In some instances, international conventions, such as the conventions developed by the Hague Conference on Private International Law, will apply, provided that both the EU/EU member states and the United Kingdom are parties to the convention.

Establishing a business

5 What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

The requirements and procedures which govern the establishment of a digital business are the same as those that govern the establishment of brick-and-mortar businesses. Individuals choosing to operate as a sole trader should register with HMRC and those deciding to establish a company should register that company at Companies House. It is important to ensure that any name chosen for the business is available and does not infringe any pre-existing third party intellectual property (IP) rights. The domain name of any website the business will use must be registered. If relevant, the necessary business permits, licences and authorisations should be obtained (eg, a digital business offering payment services or financial advice would need to be registered with, or approved by, the FCA). Once a digital business is established in the United Kingdom, the person responsible for the business must ensure compliance with:

- the GDPR;
- the Privacy and Electronic Communications Regulations 2003 (as amended);
- the Electronic Commerce Regulations 2002 (as amended); and
- the Consumer Protection (Distance Selling) Regulations 2000 (if relevant).

© Law Business Research 2019

CONTRACTING ON THE INTERNET

Contract formation

6 | Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

Yes, it is possible to form and conclude contracts electronically. Standard English law contract principles of offer and acceptance apply equally to contracts formed electronically. In order to avoid possible demand issues, it is important that people selling online structure their sites in a way that ensures that the site content is not viewed as an 'offer' that can be accepted by any buyer, but rather as an 'invitation to treat' (ie, like a shop window). The buyer is then the party that makes the offer that the seller is at liberty to accept or reject. This can be an important distinction in cases of pricing errors.

In order to avoid issues regarding whether or not acceptance has actually taken place, at which time a contract is in force between the parties, the Electronic Commerce (EC Directive) Regulations 2002 apply to internet contracts to ensure that when placing an order on the internet, a receipt is provided and the customer has the opportunity to identify and correct errors prior to placing the order. It is also a requirement of the Directive that the service provider provides terms and conditions applicable to the contract to the customer in a way that the customer may store and reproduce them. It is currently unclear what the position will be when the United Kingdom exits the European Union; this will depend upon whether the United Kingdom exits with or without a deal.

Most websites seek to enforce terms and conditions of use on users by means of a 'click wrap' or 'click through' contract, usually in the form of a screen containing the terms and conditions of use which are available to read and to either accept or reject.

The click wrap concept follows the shrink wrap contract or licence that has been commonly used in the software industry since the 1980s. Two cases in 1996, *Beta Computers (Europe) Limited v Adobe Systems (Europe) Limited* under Scottish law and *Pro CD Inc v Zeidenberg* under US law, have both enforced the validity of shrink-wrap licence agreements, provided the customer has the opportunity to read and if necessary reject the terms by returning the product within a reasonable period. In the case of click wrap contracts, the same principles need to apply.

The Unfair Contract Terms Act 1977 (as amended) applies to any click wrap terms and conditions so that any terms must be fair and reasonable, particularly those that seek to limit liability.

Applicable laws

7 | Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

In addition to English common law principles that apply to contracting on the internet, the main laws that govern contracting on the internet have been mentioned above and several of them specifically relate to business-to-consumer transactions while not applying to business-to-business transactions, an example being the CRA, which only applies to consumer transactions. The Electronic Commerce (EC Directive) Regulations 2002 also apply to contracting on the internet; however, they apply to any natural person who is acting for purposes other than those of his or her trade, business or profession.

The Unfair Contract Terms Act 1977 can apply to consumer-to-business contracts and also to business-to-business contracts, provided that one party deals 'on the other's written standard terms of business'.

Two new EU directives proposing to harmonise the rules on digital contracts across the European Union are currently passing through the EU's legislative process:

- the Supply of Digital Content Directive; and
- the Sale of Goods Directive.

The Supply of Digital Content Directive concerns contract rules on the supply of digital content and would govern business-to-consumer contracts formed online. The Directive covers all contracts between traders and consumers concerning the supply of digital content (data supplied in digital form, including software, video, audio and e-books) and the provision of digital services (including cloud computing, social media, data-sharing and online work tools). The Sale of Goods Directive concerns contract rules on the online sale of goods. It is anticipated that these Directives will be approved by the European Parliament in 2019. It is unclear whether they will be applicable to the United Kingdom; this depends on whether the United Kingdom exits the European Union with or without a deal.

Electronic signatures

8 | How does the law recognise or define digital or e-signatures?

Electronic signatures have long been recognised as legally valid in the United Kingdom. For example, in *Hall v Cognos Ltd* ET/1803325/97, where a contract stated that any variation must be in writing and signed by the parties, it was found that the exchange of emails between employer and employee was 'in writing' and that the printed name on top of the email along with a signed first name was a sufficient signature.

At EU level, the aim of Regulation (EU) No. 910/2014 on electronic identification (the eIDAS Regulation) was to improve on the previous framework for electronic signatures which suffered from a lack of consistency, uptake and confidence. The Regulation distinguishes between simple electronic signatures, which include a name on the bottom of an email, a scanned signature or ticking 'I agree' on a website, and qualified and advanced electronic signatures, which follow a more formalised standard. The Regulation has strengthened the legal effect of simple electronic signatures across the member states. Electronic signatures may be used by individuals but not by organisations. Organisations should use 'electronic seals'. However, individual authorised signatories may still use simple electronic signatures to bind companies in accordance with corporate law.

In the event that the United Kingdom exits the European Union with a deal, the United Kingdom will continue to recognise existing EU rules on digital or e-signatures – they will be retained in an amended form under domestic law by means of the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc) (EU Exit) Regulations 2018. This instrument amends provisions that are inappropriate or redundant as a result of the withdrawal of the United Kingdom from the European Union. These amendments include changes to terminology and removing requirements which will no longer be appropriate post-EU exit, (eg, a requirement for member states to notify the European Commission of the trusted list provider). The intention for trust services (including services relating to electronic signatures, electronic seals, timestamps, electronic delivery services and website authentication) is to ensure continued mutual recognition and interoperability with the European Union is still possible.

Data retention

9 | Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

There are no particular record-keeping requirements in relation to the formation of electronic contracts. Each party is, however, well advised

© Law Business Research 2019

to maintain an audit trail in the event of a dispute arising as to the terms of the contract or its performance within the six years' statutory limitation period.

Further, mandatory disclosure requirements under consumer laws mean that traders have to keep at least minimal records of the information provided to consumers at the time of transactions in order to demonstrate their compliance with those requirements.

Breach

10 | Are any special remedies available for the breach of electronic contracts?

There are no special remedies available for the breach of electronic contracts in the United Kingdom. The usual remedies for contractual breach are available (eg, damages, specific performance and injunction).

SECURITY

Security measures

11 | What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

The Privacy and Electronic Communication Regulations 2003 (PECR) (as amended) (see question 34), the NIS Regulations (see question 35) and the Communications Act 2003 impose an obligation on the providers of public electronic networks to put in place appropriate technical and organisational measures to safeguard the security of the service.

Common law principles and non-internet-specific legislation may also apply. For example, a company that loses or permits unauthorised third-party access to customer data may, for example, face a claim for negligence, breach of contract (if there was a contractual term to take care of such data) and a claim under the GDPR, on the basis that such loss or unauthorised access is likely to be a breach of the GDPR's 'integrity and confidentiality' data protection principle that requires personal data to be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The British Standard, BS 10012:2017 (as amended), provides a specification for a personal information management system. This standard provides guidance on how to ensure compliance with the requirements of the GDPR. Although not specifically targeted at internet transactions, it is the only standard prescribing a personal information management system that is compatible with current data protection legislation.

In 2014, the government introduced the Cyber Essentials scheme, which sets out the basic controls that all organisations should implement to mitigate the risk from internet-based threats, and concentrates on five 'key controls':

- boundary firewalls and internet gateways;
- secure configuration;
- access control;
- malware protection; and
- patch management.

The scheme provides guidance to organisations on the implementation and offers independent certification.

More generally, data protection legislation imposes an obligation to put in place appropriate technical and organisational measures to safeguard 'personal data'. Given the broad definition of the term, which includes most transactional data, this requirement has created a framework for cybersecurity measures across all industries. Under the GDPR, data controllers and data processors alike have to implement appropriate technical and organisational security measures to protect personal data, including, where appropriate:

- pseudonymisation;
- encryption;
- the use of confidentiality ensuring systems;
- integrity and processing resilience;
- data backup; and
- disaster recovery systems.

The regulation provides scope for the development of an approved code of conduct and/or approved certification mechanism to demonstrate compliance with the GDPR's security requirements. The UK government has stated its intention to transpose the GDPR into domestic law via the EU (Withdrawal) Act 2018 (EUWA 2018) even in the event of a no-deal Brexit, however, to ensure the UK data protection framework continues to operate effectively when the United Kingdom is no longer an EU member state the government will make appropriate changes to the GDPR and the Data Protection Act 2018 using regulation-making powers under EUWA 2018.

Encryption is not expressed to be a mandatory requirement under legislation. However, on the basis of commonly adopted security measures and trends in enforcement action by data protection regulators, we can safely assume that encryption is a mandatory requirement under data protection law for most cases of storing of personal data on portable devices, in electronic files, such as ZIP files, for emails used to transfer large amounts of third-party personal data, and for storing of consumer data.

Government intervention and certification authorities

12 | As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

The Investigatory Powers Act 2016 maintains the government's ability to request access to private communications with a warrant. In addition, pursuant to the Investigatory Powers (Technical Capability) Regulations 2018 enforcement agencies are able to serve 'technical capability notices' on telecommunications operators or postal operators in order to ensure that the operator has the capability to provide assistance in relation to interception warrants, equipment interference warrants, or warrants or authorisations for the obtaining of communications data.

eIDAS Regulation (EU) No. 910/2014 requires member states to cooperate in order to reach interoperability and security of electronic identification schemes. The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 designate the ICO as the regulator for electronic identification and trust services for electronic transactions.

Under current proposals, the United Kingdom will lose access to the EU's interoperability system and to the underlying EU information systems when it exits the European Union (regardless of whether it exits with or without a deal). Since the United Kingdom will no longer have access to the interoperability framework for electronic identification provided by the eIDAS Regulation, it intends to repeal the electronic identification sections of the eIDAS Regulation via the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc) (EU Exit) Regulations 2018.

© Law Business Research 2019

Electronic payments

13 | Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

In the United Kingdom, electronic payment systems and services are governed by the Electronic Money Regulations 2011 (as amended) and the Payment Services Regulations 2017 (as amended). The providers and operators of electronic payment systems are regulated by the FCA, the PRA and the Payment Systems Regulator (PSR). The rules and restrictions are applicable to UK businesses providing payment services and/or issuing e-money in the United Kingdom as a regular occupation or business activity. These businesses must be authorised or registered by the FCA. There are no specific rules or restrictions for digital businesses making use of electronic payment systems provided by other businesses, but these digital businesses may want to consider the security of their chosen electronic payment systems and comparative costs to the business of different systems providers.

14 | Are there any rules or restrictions on the use of digital currencies?

There is currently no UK legislation that directly regulates the use of digital currencies, such as Bitcoin. Digital currencies do not fit squarely within the existing financial regulatory regimes in the United Kingdom either. In 2018, the House of Commons Treasury Committee undertook an inquiry into UK digital currencies, publishing a report in September 2018, which indicated that the Committee considered that the UK government and regulators' position on crypto-assets was ambiguous and recommended regulating the 'Wild-West' of crypto-assets. The report did not, however, specify how the recommended regulation should be achieved. The EU's fifth Anti-Money Laundering Directive, which entered into force on 9 July 2018 and imposes certain obligations in respect of crypto-asset exchanges, marks the beginnings of the introduction of a regulatory framework with respect to digital currencies. However, EU member states have until January 2020 to amend their national laws to align with the new AML Directive and it is unclear whether the United Kingdom will do so before exiting the European Union.

DOMAIN NAMES

Registration procedures

15 | What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

The rules for the registration and use of domain names within the '.uk' domain and its subdomains are administered by Nominet UK. Applications to register a domain name will generally be made on behalf of an applicant by a registrar (generally an internet service provider (ISP) or registration agent). Prices will vary depending on which registrar is used and registrations are for a period between one and 10 years before renewal is required. Domain names can be transferred from one entity to another, subject to payment of a fee (at present £10 plus VAT for any number of domains transferred) to Nominet UK.

It is possible to register a '.uk' domain name without being resident in the United Kingdom, subject to certain restrictions in respect of '.plc.uk' and '.ltd.uk' names, where the registrant must be either a private or public company registered as such with Companies House. '.biz' domain names are intended to be used by businesses. These can be registered by anybody and there are no specific information requirements to create a '.biz' domain name.

Rights

16 | Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

Domain names in themselves do not provide a great deal of protection against third parties using the same or similar names, particularly when initially registered, when no goodwill may have attached to a particular name. If, however, the domain name is also the registrant's trademark, then evidence as to visitor numbers to the domain name in an infringement or opposition action against a third party would be useful. In the absence of a registered trademark, or as an additional claim in a trademark infringement claim, it is conceivable that the owner of a particularly well-known domain name might be able to establish sufficient reputation in a domain name to successfully bring a passing-off claim if a third party's use of a well-known domain name was such as to lead the public into the erroneous belief that there is a connection between the domain name owner and the third party.

Trademark ownership

17 | Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

Yes, depending on the precise circumstances of each 'cybersquatting' case and the way in which the 'pirate' conducts itself, it may well have a bearing on the outcome. In *British Telecommunications v One in a Million* [1999], several owners of well-known trademarks were successful in bringing a passing-off claim on the grounds that the registration of the domain name and the subsequent offer of sale to the claimants made a false representation that the defendant was associated with the claimant, and potentially raised the prospect of damage to the claimants if they did not purchase the domain names offered to them. In the same case, with regard to trademark infringement, the court ruled that the defendant's use of the claimants' well-known trademarks (which had a reputation in the United Kingdom) was detrimental to the reputation of the marks and amounted to trademark infringement under the Trade Marks Act 1994. There are other examples of successful claims by trademark owners, although it is worth noting that there have also been cases where the courts have found that a domain name registrant has a perfectly legitimate right to register a domain name, particularly where the goods and services differed from those of the trademark owners and there was therefore no likelihood of confusion.

As an alternative to court action, a trademark owner may decide to use the more informal procedures offered by the Internet Corporation for Assigned Names and Numbers (ICANN) with respect to top-level domain names or Nominet UK in respect of '.uk' domain names. This is often a cheaper and quicker route to resolution than court action and can be particularly useful where the aim is to achieve transfer of the domain name rather than pursue damages.

Dispute resolution

18 | How are domain name disputes resolved in your jurisdiction?

Nominet, the .uk domain name registry in the United Kingdom, provides a dispute resolution service. A person wishing to make a complaint about a .uk domain name must submit a complaint through the Nominet Online Services tool on the Nominet website by filling out a complaint form. Nominet will then send a copy of the complaint to the registrant of the domain name, who has a set time period within which to respond. If the registrant does not agree to the remedy requested by the complainant, Nominet offers a free mediation services. However, mediation is voluntary. If the registrant does not respond or if it is not possible to settle the case by mediation, the complainant has the option of paying a fee to appoint an independent expert to make a binding decision about

© Law Business Research 2019

what should happen to the domain name. It is possible to make an appeal against an expert decision, although appeals are uncommon.

ADVERTISING

Regulation

19 | What rules govern advertising on the internet?

Advertising on the internet is governed by the same rules that apply to other advertising channels, although the reach of the internet poses potential problems for advertisers where their ads may be viewed further afield than might be intended. Advertisers would be well advised to clearly state at which jurisdiction their ads are aimed.

In the United Kingdom, advertisers need to comply with the Business Protection from Misleading Marketing Regulations 2008, which prohibit misleading advertising to businesses and establish when comparative advertising will be allowed. Advertisers also need to comply with the Consumer Protection from Unfair Trading Regulations 2008 (as amended) under which commercial communications made to consumers that are misleading or aggressive are prohibited.

Additionally, advertisers need to comply with the British Codes of Advertising, Sales Promotion and Direct Marketing (as published by the Committee of Advertising Practice and known as the CAP Code) that have been found to apply to internet activities. The ASA has responsibility for enforcing the CAP Code. The CAP Code applies to advertisements, promotions, the content of organisations' own websites and advertising and marketing on social networking sites. The CAP has provided guidance on specific sectors such as comparative charity ads, adult material and betting tipsters. In February 2019, the ASA published new (and more restrictive) standards for advertising gambling.

Further, specific rules on advertising apply to certain specific sectors, such as the financial services sector where advertising has to comply with the FCA Handbook.

The Gambling Act is an example and contains specific rules relating to the advertising of gambling activities.

Definition

20 | How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

This will depend on the content of the communication. Genuine lawful editorial content will be subject to journalistic exemptions which will defeat any claims of defamation, infringement of intellectual property, breach of personal data laws or advertising laws. However, editorial content which is also intended for advertising may not escape these claims. Under the CAP Code, marketing communications must be obviously identifiable as such.

Misleading advertising

21 | Are there rules against misleading online advertising?

The ASA enforces the CAP Code, which requires that marketing claims are substantiated and evidence has to be kept by the advertiser. Misleading advertising is a criminal offence under the Consumer Protection from Unfair Trading Regulations 2008 (as amended) as well as the Business Protection from Misleading Marketing Regulations 2008.

Restrictions

22 | Are there any products or services that may not be advertised on the internet?

While no products are entirely banned from advertisement on the internet, UK laws regulating advertisements for, among others, alcohol, tobacco, lotteries, food and drink, and prescription drugs will apply to the internet. Tobacco advertising in particular is heavily regulated by the Tobacco Advertising and Promotion Act 2002 and the exceptions to a general prohibition are limited. Additionally, the ASA has published rules as part of the British Code of Advertising, Sales Promotion and Direct Marketing relating to non-broadcast advertisements for food or soft drink products aimed at children and non-broadcast advertisements relating to gambling with the implementation of the Gambling Act 2005. Such advertisements are not banned but must satisfy certain requirements of the code, such as the requirements not to be misleading or cause harm and offence. In particular, marketing communications to children must not encourage or otherwise condone poor nutritional habits or an unhealthy lifestyle in children. Gambling marketing must also ensure that the marketing is socially responsible, with a particular responsibility to persons under 18, children and other vulnerable persons. In February 2019, the ASA published more restrictive standards for advertising gambling.

Hosting liability

23 | What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

Content providers are primarily liable. ISPs can rely on the 'mere conduit' defence under the Electronic Commerce (EC Directive) Regulations 2002 that applies to mere hosting or caching of information. Website operators may rely on a similar defence under the Defamation Act 1996 and 2013 to defeat any defamation claim (see questions 20 and 22).

Although The Electronic Commerce (Amendment etc) (EU Exit) Regulations 2019 (SI 2019/89) will amend the Electronic Commerce (EC Directive) Regulations 2002 and the EC Directive (Miscellaneous Provisions) Regulations 2018 when the United Kingdom exits the European Union, these defences (implemented in domestic law) will continue to apply and the United Kingdom intends for the UK and EU positions on e-commerce to continue to be aligned.

FINANCIAL SERVICES

Regulation

24 | Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

Since 2012, financial services have been regulated by the FCA and the Prudential Regulation Authority. The FCA took over responsibility from the Financial Services Authority for the requirements relating to financial promotions conduct of business regulation of the UK financial services industry. The FCA's financial promotion regime is intended to be media-neutral. This means that publications on the internet are treated in the same way as documents published in newspapers or posted to recipients. The FCA's rules therefore focus on the content of the financial promotion rather than the medium used to communicate it. The FCA has the power to require firms to withdraw or amend a misleading financial promotion with immediate effect and to announce that it has done so.

By law most financial services business operating in the United Kingdom require authorisation from the FCA under the Financial Services and Markets Act 2002. Matters concerning 'non-technical' elements of financial advertisements, such as taste and decency or social responsibility, are regulated by the ASA.

Companies advertising financial products or services must ensure that their ads (which can include emails and websites) are clear and fair and do not mislead customers. Customers are encouraged to report misleading ads and unfair terms in customer contracts to the FCA.

© Law Business Research 2019

A key piece of legislation regarding the online marketing of financial services in the United Kingdom is the Financial Services (Distance Marketing) Regulations, which came into effect in October 2004 and implemented the 2002 EU Directive on the Distance Marketing of Financial Services. The Regulations only apply to consumer contracts concluded at a distance and require the supplier to disclose certain information, including the supplier's geographical address and particulars of any supervisory body (eg, the FCA) with a link to their website, together with information as to the product details and the terms of the contract, including right to cancel and payment details. Consumers have the right to cancel without incurring liability within a specified cooling off period in most cases (but not all), the length of which will depend on the nature of the product. The information required must be provided to the consumer in a clear and comprehensible manner on paper or another appropriate durable medium before the contract can be concluded. The supplier must provide a copy of its terms and conditions prior to conclusion of the contract. The Financial Services (Distance Marketing) (Amendment) (EU Exit) Regulations 2019, which will come into force when the United Kingdom exits the European Union, will amend the UK regulations to ensure that they continue to operate effectively in the United Kingdom once the United Kingdom has left the European Union. It is currently unclear what the position will be in the event of a no-deal Brexit, but it is likely that the United Kingdom will adopt the same approach, albeit that the amendment of these regulations may be subject to some delay.

DEFAMATION

ISP liability

25 | Are ISPs liable for content displayed on their sites? How can ISPs limit or exclude liability?

In *Godfrey v Demon Internet* [1998], Demon (an ISP) was held liable for defamatory material that it failed to remove for a period of 10 days after being advised that the material was defamatory. Given the Court of Appeal's recent decision in *Tamiz v Google Inc* [2013], where it was found that Google was a publisher once it had been notified of certain defamatory comments posted on its blogging platform, ISPs should therefore remove material that might be defamatory as soon as possible on being informed of such material.

However, the Defamation Act 1996 provides for a defence for ISPs that act as an 'intermediary'. The Defamation Act 2013 provides for a defence for website operators. The Defamation Act 2013, as supplemented by the Defamation (Operators of Websites) Regulations 2013/3028, also provides a specific defence for operators of websites in defamation proceedings. Intermediaries or ISPs that provide 'information society services' may also be able to rely on a range defences under the Electronic Commerce (EC Directive) Regulations 2002 (as amended) to defend against defamation actions (see question 18). In December 2018, in *Magyar Jeti ZRT v Hungary*, the European Court of Human Rights (ECHR) found that the company operating the news website 444.hu was not liable for putting a hyperlink to another publisher's defamatory video in an online article on its platform. The ECHR acknowledged that an ISP could be liable for hyperlinking to defamatory third-party content, but stated that the test was subjective (not objective) and liability would depend upon the facts.

The Electronic Commerce (Amendment etc) (EU Exit) Regulations 2019 (SI 20019/89) will amend the Electronic Commerce (EC Directive) Regulations 2002 and the EC Directive (Miscellaneous Provisions) Regulations 2018 when the United Kingdom exits the European Union, meaning that the provisions therein (implemented in domestic law) will continue to apply and the United Kingdom's approach will be aligned with that of the European Union. However, it is currently unclear what the position will be in the event of a no-deal Brexit.

The European Union's new Copyright Directive, which was recently approved by the European Parliament, marks a significant overhaul of copyright law in the European Union. As part of the changes, hosting platforms – such as YouTube – will be legally responsible for the user-generated material they host in the European Union. All platforms will be required to take out licences with rights holders to show their material. Platforms must use their 'best efforts' to remove copyrighted material if they are alerted to pirated uploads. At the time of completing this note, it is unclear under what circumstances and when the United Kingdom will exit the European Union and consequently whether it will implement the new Copyright Directive in domestic law.

Shutdown and takedown

26 | Can an ISP shut down a web page containing defamatory material without court authorisation?

No, unless it can rely on clear terms and conditions that state that the ISP has such rights of removal, even in the case of an allegation of defamation. However, ISPs would be best advised to investigate the matter quickly and thoroughly before taking such action. The ISP may also wish to consider including in its terms an indemnity in its favour if damages are sought against it as part of a defamation claim.

INTELLECTUAL PROPERTY

Third-party links, content and licences

27 | Can a website owner link to third-party websites without permission?

The issues with regard to third-party content used on the internet will be the same as if they were used in other contexts, the primary question being whether the third-party content in issue is protected by copyright (or possibly other rights such as database, trademark or design rights). If the content being used is protected by copyright (or other rights), then use without permission will, subject to certain limited exceptions and assuming that such use amounts to the copying of the whole or a substantial part of the copyright work or otherwise constitutes an act that is reserved for the copyright owner and his or her authorised users, be an infringement and expose the website provider to a claim for copyright infringement. Depending on the facts, a claim in passing off may also be established.

Simple linking without permission from one homepage to another homepage where there is no copying of any copyright material is acceptable, although the owner of a linked site could theoretically claim that a link causes a breach of the 'making available right' introduced into UK law by the Copyright and Related Rights Regulations 2003, if it could be shown that the link constitutes an 'electronic transmission in such a way that members of the public may access the copyright work from a place and a time individually chosen by them'. Using a third party's trademark or copyright work as part of the link could also raise issues. The party creating the link should also bear passing-off and trademark issues in mind when creating the link and should make it clear that the user is leaving one site and going to another. Linking in breach of a contractual obligation not to do so might also constitute a breach of contract.

Deep-linking (bypassing the homepage of the linked site) raises similar concerns for sites linked without permission. Arguments have been run successfully against deep-linking in other EU jurisdictions based on infringement of database rights. A claimant would need to show that the relevant pages on its website constituted a database and that the link made the database available in a manner that constituted reutilisation. Deep-linking may be more objectionable from the rights holders' perspective.

© Law Business Research 2019

'Framing' is the practice of displaying content from another website within the frame or border of a website. As framing involves copying another party's content, the risk of a copyright infringement claim is greater than with linking if the framed content constitutes a substantial part of the framed website's copyright material. Additionally, depending on the precise circumstances of the case, the framing party potentially runs the risk of a passing-off claim, a trademark infringement claim, a database rights infringement claim and a breach of contract claim.

A further issue that has been of interest in this respect in the United Kingdom is the use of 'metatags' (also known as 'keywords') whereby website providers seek to drive traffic to their sites by the use of other party's trademarks in the embedded code of their sites that is then picked up by a search engine searching against that term. In the case of *Interflora Inc and another v Marks and Spencer plc and another* [2013], it was held that Marks and Spencer had infringed Interflora's trademark by purchasing 'Interflora' AdWords, which led customers who ran a search for 'Interflora' to believe that Interflora was part of Marks and Spencer's flower delivery service. Since the decision turned on its facts, however, it is not clear to what extent other trademark owners will be able to draw comfort from this decision. Nonetheless, this decision means that a certain amount of care needs to be taken in this regard, and a trademark owner that feels that its marks are being taken advantage of may wish to complain to the search engine in question, even if it decides not to take more formal legal action.

28 | Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

Generally, this will not be permitted subject to limited exceptions, such as the journalistic exception. Copyright infringement attracts civil as well as criminal liability. A copyright owner could commence private criminal prosecution of a website operator that has copied copyrighted material.

29 | Can a website owner exploit the software used for a website by licensing the software to third parties?

This will largely depend on who owns the copyright (and, if relevant, the database rights) in the relevant software, and if it is licensed in by the website provider, and whether sub-licensing is permitted by the terms of its licence.

If the website provider is not the owner of the rights in the software and it is not expressly permitted to sub-license the software to a third party, then such sub-licensing may expose the website provider to a claim for breach of contract and a copyright (and possibly database rights) infringement claim, as well as expose the purported sub-licensee to a copyright (and possibly database rights) infringement claim by the actual owners of such rights.

30 | Are any liabilities incurred by links to third-party websites?

Website providers providing links to third-party websites will generally provide an express statement at the point of the link stating that the user is moving from one site to another and that no liability is accepted for the content of the site being linked to or for the user's use of the linked site. The question to be answered would most likely be whether such an exclusion was reasonable under the Unfair Contract Terms Act 1977 and additionally, where the user is a consumer, whether the exclusion was fair and reasonable under the Unfair Terms in Consumer Contracts Regulations 1999.

In *McGrath v Dawkins* [2012] the High Court considered that a website operator could be liable for defamation on the basis of linking to defamatory content on another website. In December 2018, in *Magyar Jeti ZRT v Hungary*, the ECHR found that the company operating the news website 444.hu was not liable for putting a hyperlink to another publisher's defamatory video in an online article on its platform. The ECHR acknowledged that an ISP could be liable for hyperlinking to defamatory third-party content, but stated that the test was subjective (not objective) and liability would depend upon the facts.

In the past few years, there have been a number of European Court of Justice (CJEU) decisions concerning copyright liability for various forms of hyperlinking, for example, in *Pirate Bay* (Case C-610/15) the CJEU assessed the use of 'magnet links' to download illegal content from peer-to-peer file-sharing sites and in *Filmspeler* (C-527/15) the Court assessed the use of hyperlinks embedded in add-ons loaded onto a physical multimedia player. Although these decisions turned on the facts of each case they have expanded the scope of the communication to the public right under the InfoSoc Directive 2001/29/EC so that broader groups of website and platform operators that link to illegal content may now be regarded as primarily liable for unauthorised acts of communication to the public. In *GS-Media v Sanoma* (C-160/15) the CJEU held that providing a hyperlink to freely accessible online content posted without the consent of the copyright owner could constitute a copyright infringement if the person placing those links knew this consent was not given. The link itself could also give rise to a trademark infringement or other claims by the owner of the site to which a link is provided.

Video content

31 | Is video content online regulated in the same way as TV content or is there a separate regime?

Television-like programmes, such as TV programmes or video on demand services that are accessible online, are subject to the Audiovisual Media Services Directive implemented by the Communications Act 2003 and subject to regulation by Ofcom. Other online video content, such as some YouTube content, is currently not subject to this regime; the applicability of the Audiovisual Media Services Directive to online video content primarily currently turns on whether the operator of the relevant website or online platform exercises editorial control over the content. However, in November 2018, the EU Council approved amendments to the Audiovisual Media Services Directive, such that online platform providers like Facebook and YouTube must soon adhere to the EU's revised Audiovisual Media Services rules. EU member states have until September 2020 to implement the new rules; whether the United Kingdom will implement these changes is currently uncertain.

IP rights enforcement and remedies

32 | Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

Under the Copyright, Designs and Patents Act 1988 authorities have the power to enter premises and inspect and seize goods and documents in connection with criminal copyright and design offences.

33 | What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies in relation to most IP rights include delivery up, damages, account of profit, injunction, search orders and freezing injunctions in order to secure payment of damages.

© Law Business Research 2019

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

34 | How does the law in your jurisdiction define 'personal data'?

Under the GDPR, 'personal data' is defined as any information relating to an identified or identifiable natural person who can be identified directly or indirectly by reference to an identifier, such as a name or identification number or by reference to one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Given this broad definition, even personal data that has been anonymised could potentially remain personal data, especially if other data that could be used to identify individuals is in the public domain or the controller retains the key for reversing the anonymisation.

The GDPR refers to special categories of personal data which broadly correspond to the category of sensitive personal data under the previous legislative regime. The special categories of data consist of information as to:

- the racial or ethnic origin of the data subject;
- his or her political opinions;
- religious belief;
- philosophical beliefs;
- his or her trade union membership;
- his or her physical or mental health; and
- sexual life or sexual orientation.

Specific additional conditions for processing special category data are set out in article 9(2) of the GDPR. Information concerning the commission or alleged commission of a criminal offence, or any proceedings for any criminal offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings is not included within the categories of special personal data, but specific safeguards for processing such data are set out in article 10.

Under the GDPR, psyeudonymised data is still personal data that falls within the scope of the GDPR. However, the GDPR does not apply to data that has been anonymised. In order for data to be truly and effectively anonymised under the GDPR, the individual to whom the personal data relates must no longer be identifiable.

Note: DPA 2018 did not transpose the GDPR into UK law. The UK government intends to transpose the GDPR into domestic law through the Withdrawal Agreement if the United Kingdom exits the European Union with a deal. At the time of writing, it is uncertain whether this will be the case and whether, if the United Kingdom leaves the European Union without a deal, the GDPR will be immediately transposed into UK law.

Registration requirements

35 | Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioners Office (ICO), unless they are exempt. This duty replaces the requirement to 'notify' or register under the Data Protection Act 1998. There are three different levels of fee to pay depending on the size of the organisation. Exemptions are limited and include organisations that only process personal data for:

- staff administration;
- advertising;
- accounts;
- judicial functions; and
- personal, family or household affairs.

It is mandatory for certain data controllers and data processors to designate a data protection officer (DPO). This includes any public authority or public body that handles data and any other organisation that conducts 'regular and systematic' monitoring of individuals on a 'large scale' or where an organisation's core activities involve the processing of special categories of (ie, sensitive) personal data on a large scale. Equally, the new law does not prevent other organisations not required to designate a DPO from doing so on a voluntary basis (eg, where the organisation in question finds it useful to do so). Indeed, the guidance of the Article 29 Working Party encourages voluntary designation of DPOs.

In terms of enforcement, the GDPR has introduced new, extensive sanctions including a new monetary penalty regime for non-compliance which increases the penalty thresholds to the greater of 4 per cent of annual worldwide turnover or €20 million. Fortunately, not all infringements will incur the maximum fines as the level of fine will be determined by the nature, gravity and duration of the relevant infringement. In addition to administrative fines, the GDPR gives local data protection authorities the power to issue warnings, reprimands and orders. Each local data protection authority is likely to develop an enforcement policy within the boundaries of the GDPR so moving forward companies should be cautious of the ICO stepping up its enforcement activities and using its enhanced fining powers more readily.

Companies that are FCA-regulated should also be aware that the FCA can impose unlimited fines for data breaches; in August 2018, the FCA fined Tesco Bank £16.4 million for data security failings in relation to a 2016 cyber-attack.

Cross-border issues

36 | Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

A key change to the regulatory landscape comes with the extended jurisdiction of the GDPR, which now applies to all companies processing the personal data of data subjects residing in the European Union, regardless of whether the company itself is located within the European Economic Area. Equally, the GDPR is clear that it applies to the processing of personal data by controllers and processors in the European Union regardless of whether the processing takes place in the European Union or not. With the introduction of GDPR, non-EU companies will also have to appoint a representative responsible for data processing in the European Union.

Given the extra-territorial effect of the GDPR, when the United Kingdom exits the European Union (with or without a deal), the GDPR will continue to apply to any online businesses based in the United Kingdom that are processing the personal data of citizens based in the European Union and these companies may need to appoint a representative responsible for data processing in the European Union.

In the event of a no-deal Brexit scenario, the UK government intends to retain the extraterritoriality of the UK's data protection framework. The UK data protection framework will apply to controllers or processors who are based outside the United Kingdom where they are processing personal data about individuals in the United Kingdom in connection with offering them goods and services or monitoring their behaviour. This includes controllers and processors based in the European Union. Such controllers, based outside of the United Kingdom, will need to appoint a data protection representative in the United Kingdom.

As far as possible, the UK government intends to preserve the current position on personal data transfers from the United Kingdom to the European Economic Area and non-EEA countries in the event of a no-deal Brexit scenario. The UK government has stated that it will transitionally recognise (subject to review) all EEA states, EU and EEA

© Law Business Research 2019

institutions, and Gibraltar as providing an adequate level of protection for personal data. This means that it will be possible for UK companies to continue to transfer personal data from the United Kingdom to these countries after the United Kingdom exits the European Union. However, whether or not data will be able to freely flow into the United Kingdom from EEA countries is not within the United Kingdom's control; jurisdictions outside of the United Kingdom will provide their own rules on the transfer of data internationally. The UK government has advised that UK organisations that are reliant on data transfers from the European Union should seek to rely on alternative mechanisms for such transfers, for example using standard contractual clauses.

Where the European Union has made an adequacy decision in respect of a country or territory outside of the European Union prior to exit day, the UK government intends to preserve the effect of these decisions on a transitional basis. This will mean that transfers from UK organisations to non-EEA countries deemed 'adequate' can continue uninterrupted. The list of recognised countries is available on the European Commission's website. Standard Contractual Clauses that have previously been issued by the European Commission will continue to be an effective basis for international data transfers from the United Kingdom in a 'No Deal' scenario. Existing authorisations of Binding Corporate Rules made by the Information Commissioner will continue to be recognised in domestic UK law after the United Kingdom exits the European Union.

Customer consent

37 | Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

The legal ground relied upon for processing under article 6 of GDPR will depend on the nature of the processing, the context in which the data is being processed and the relationship between the data controller and the data subject. Reliance on the ground of consent opens the controller up to extra obligations and extra rights for the data subject so is not always the best ground to rely on if there are other grounds that can be relied upon instead. Processing in relation to digital contracts may be carried out on the basis that it is necessary because of an actual or proposed contract between the individual and the data controller. Organisations can also rely on legitimate interests processing where their legitimate interests are not outweighed by the privacy rights of the individual. Other grounds of processing include processing necessary for the compliance with a legal (non-contractual) obligation, processing necessary for the performance of a task carried out in the public interest or necessary in order to protect the vital interests of a natural person (unlikely to be relevant in relation to digital contracts).

Consent is the ground mainly used for processing for new purposes, processing that is particularly intrusive, or for sharing of personal data with third parties. Consent is also required for use of cookies under PECR. The ICO cautions that consent under the GDPR requires clear affirmative action, meaning that an individual must take deliberate and specific action to opt in or agree to the processing, even if this is not expressed as an opt-in box.

The GDPR sets out specific additional grounds for the processing of special categories of data at article 9. One such additional ground is that the data subject must give explicit consent for one or more specified purposes. In order to process criminal offence data not only must organisations have a legal basis under article 6, but the processing must also be carried out only under the control of official authority or be authorised by European Union or member state law – in the United Kingdom this means complying with at least one of the additional conditions set out in Schedule 1 of DPA 2018.

Sale of data to third parties

38 | May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

A website provider that wishes to sell a database must ensure that in doing so it complies with the principles of DPA 2018 and the GDPR, in particular processing must be fair, lawful and transparent and for specified lawful purposes only. The best way to ensure that these principles are met on a sale of a database will be to include an express statement in the website's privacy policy stating that sale of the database to a third party is a possibility, whether as a sale of the website provider or as part of the website operator's general business. Further, where sale is to a third party for the direct marketing purposes of the third party, the website provider should seek an explicit consent to the transfer of data to a third party for direct marketing purposes. Consent to be contacted by 'selected partners from time to time about products that may be of interest to you' will generally not suffice. If such consent is not obtained, then the data subject's information should not be included within the database on sale. The ICO has published updated guidance on direct marketing under the GDPR, DPA 2018 and PECR.

If the database containing personal data is to be sold to an individual or organisation outside of the European Union, Chapter V of the GDPR only allows such a transfer to third countries where the European Commission has decided that the country, territory, sector within that country, or individual organisation ensures an adequate level of protection. If the European Commission has not determined that these criteria are fulfilled or other appropriate safeguards, such as the implementation of the European Commission's standard data protection clauses, are not provided, then personal data should not be included within the database on sale.

After the United Kingdom exits the European Union, UK organisations and individuals seeking to buy EU databases containing personal information should ensure that they have adequate protections in place as the United Kingdom will become a 'third country'. It is hoped that the European Commission will recognise the United Kingdom as providing adequate protections, however, it will not start its assessment until the United Kingdom has officially left the European Union. In the event of a no-deal Brexit scenario, the UK government intends to respect pre-existing EU adequacy decisions in respect of a country or territory outside of the European Union, preserving the effect of these decisions for the time being. This means that transfers of data from UK organisations to those countries deemed adequate can continue uninterrupted. The UK government will also continue to recognise the standard contractual clauses that have previously been issued by the European Commission and these will continue to be an effective basis for international data transfers from the United Kingdom in a no-deal scenario.

Customer profiling

39 | If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

PECR (as amended) is of importance regarding profiling by website providers of its customer base for advertising purposes. One method of collecting useful information is through the use of cookies, web bugs and other such tracking devices.

A user's informed consent is required for cookies to be used. However, the government has advised in guidance that informed consent does not have to be 'prior consent' as was originally believed by the industry. For informed consent to be obtained, the user must be presented with clear and comprehensive information of how and why

© Law Business Research 2019

any cookie is being used. Provided that sufficient information is given to the user, consent can be constituted by the user amending their browser settings to constitute consent, or by 'some other method' (new regulation 6(3A)). Note that the ICO has advised that where sufficient information is not provided, browser systems are not sophisticated enough at present for website hosts to assume that the user has given their consent for the website to use a cookie. The government has, however, given guidance to state that provided that sufficient information is clearly presented to the user (about cookies and what browser setting means for it), in some circumstances the user can actually not amend their browser settings and still be able to signify consent. The more prominent the placement of cookie information the more likely it is that the website operator will be able to assume that users understand and accept how the site works. Any attempt to gain consent that relies on users' ignorance about what they are agreeing to is unlikely to be compliant. To be valid, consent must not only be informed, but freely given and specific. It does not necessarily have to be explicit but must involve some form of unambiguous, clear and positive action (eg, ticking a box or clicking a link), the United Kingdom follows an opt-In approach to the use of cookies.

Regulation 6(4)(b) states that consent will not be required where a cookie is 'strictly necessary' to deliver a service which has been explicitly requested by the user. However, the ICO's guidance advises that the exception must be interpreted narrowly. It explains that the use of the phrase 'strictly necessary' means that its application must be limited to a small range of activities and the use of the cookie must be related to the service requested by the user (eg, the use of a cookie in relation to an online shopping basket). The idea that the services must be 'explicitly requested' by the user means that the narrowing effect of the word 'explicitly' must be borne in mind. This means that the exception would not apply 'just because you have decided that your website is more attractive if you remember users' preferences'.

Note that in relation to third-party behavioural advertising, the ICO advises that if a website uses third-party cookies in third-party behavioural advertising, that the website should 'do everything they can to get the right information to users to allow users to make informed choices about what is stored on their device'. If the information collected on a website is passed on to a third party, this must be disclosed to the user together with any options the user has. The website host should review what the third party does with any information collected.

The ICO states that it will take a practical and proportionate approach to enforcing the rules on cookies. In most cases this will involve the ICO contacting the organisation responsible for setting the cookies, asking it to respond to the complaint and requiring it to explain what steps it has taken to comply with the rules. Those breaches that continue despite the intervention of the ICO or those that are particularly privacy-intrusive are more likely to incur formal action. Where compliance is delayed because the removal of cookies in existing software requires an expensive upgrade, the ICO will expect these costs to be carefully weighed against the intrusiveness of the cookies in question and the length of time that is expected to elapse before the problem is eventually remedied. Between October 2012 and May 2016, the ICO had written to 371 organisations asking them to explain the steps they had taken towards compliance.

While the Data Protection Act 1998 focused on the outcome of automated decision-making (which includes profiling) the GDPR focuses on the act of profiling itself and introduces new rights and obligations for data subjects and data controllers respectively in relation to profiling. The new law also provides a definition of profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. The new right of individual data subjects in relation to profiling under the GDPR is the right not to be subject to a decision based on automated processing that produces a legal or significant effect on that person. This right provides the data subject with an opportunity to challenge such a decision, require human intervention in the decision-making process, obtain an explanation from the data processor, and express his or her point of view in relation to the profiling. However, it is important to note that this right cannot be exercised in relation to all scenarios, namely, individuals are unable to exercise this right in relation to:

- automated decision-making necessary for the performance of a contract;
- automated decision-making authorised by law; or
- automated decision-making based on explicit consent.

The Article 29 Working Party has published guidelines on profiling under the GDPR and this tackles some of the more nuanced issues in this area. Principally, it covers the definitions of profiling and automated decision-making and how the GDPR approaches these, the various provisions concerning profiling in the GDPR, and the impact of these provisions on processing children's personal data for profiling purposes.

Data breach and cybersecurity

40 | Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

Yes, PECR (as amended) introduced an obligation on 'service providers' (providers of public electronic services) to notify any personal data breaches to the ICO without delay. If the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or user, the service provider must also notify the individual concerned. In relation to other entities, ICO guidance states that the ICO expects that any data breaches should be made known to it. Under the GDPR, data breaches must be notified to the ICO within 72 hours. Data breaches may also need to be notified to the affected individuals who may have a right to claim compensation. Financial services firms may have further obligations to notify the FCA of any data breaches. The UK government issued guidance in March 2019 advising that in the event of a no-deal Brexit scenario, the responsibilities of data controllers across the United Kingdom will not change. GDPR standards will continue to apply in the United Kingdom and the ICO will remain the UK's independent regulator for data protection.

New reporting and notification requirements were also introduced under the EU's Second Payment Services Directive (EU) 2015/2366 (PSD2), implemented in the United Kingdom by the Payment Services Regulations 2017 (SI 2017/752) (PSR 2017). Institutions that fall within the remit of the PSR 2017 must report all major incidents (including data breaches) to the FCA within four hours of detecting the incident while the FCA is open or when the FCA re-opens. The EBA Guidelines on major incident reporting under PSD2 should be used to determine what qualifies as a major incident.

Furthermore, in mid-2016, the European Parliament adopted the NISD, which is the first piece of EU-wide legislation on cybersecurity. The NISD was transposed into national law on 10 May 2018 by the UK government. The NISD applies to operators of essential services and, importantly in relation to e-commerce, digital service providers. The directive defines digital service providers as organisations providing online marketplaces, online search engines and/or cloud computing services and an online marketplace is considered to be a service that allows consumers and traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace. Price- or product-comparison websites are specifically

© Law Business Research 2019

excluded from the meaning of an online marketplace, while an app store is given as an example of an online marketplace. Together with operators of essential services, digital service providers will be required to:

- take appropriate and proportionate technical and organisational measures to manage risks posed to the security of their network and information systems;
- take appropriate measures to prevent and minimise the impact of security incidents on their network and information systems and to ensure that those services continue to operate after such incidents, where possible; and
- notify the competent authority of security incidents, as necessary.

While the obligations on digital service providers under the NISD are less stringent than those imposed on operators of essential services, it is still important for organisations that run e-commerce offerings to ensure they are complying with this new legislation.

41 What precautionary measures should be taken to avoid data breaches and ensure cybersecurity?

The ICO provides guidance on the GDPR's security principle and what steps individuals and businesses can take to avoid data breaches and ensure cybersecurity. The GDPR requires that a person processing personal data do so securely by means of 'appropriate technical and organisational measures'; the precautionary measures that a person should take and the level of protection that the person should put in place will therefore depend upon the size of the business (and its network and information systems), its means, and the level of risk posed by the processing undertaken. Businesses should consider several factors for cybersecurity, including system security, data security, online security, and device security. The UK government's Cyber Essentials scheme, which includes a set of basic technical cybersecurity controls, could act as a starting point for deciding which cybersecurity measures are appropriate for a business; however, Cyber Essentials does not address the circumstances of every organisation or the risks posed by every processing operation and it may be necessary for a business to go beyond these requirements.

Cyber Essentials recommends:

- using a firewall for network security;
- using passwords, PINs and/or touch-ID for devices and accounts – two-factor authentication should be used for important accounts;
- only using software from official sources;
- taking anti-malware measures;
- introducing whitelisting and sandboxing;
- regularly updating devices and software; and
- managing user privileges:
    - limiting the access of staff accounts to software, settings, online services and device connectivity functions to the minimum level required for staff to perform their role;
    - limiting the number of privileged administrator accounts.

Additionally, businesses might choose to consider:

- introducing a policy to control all access to removable media;
- introducing a home and mobile working policy and training all staff to adhere to it;
- monitoring all systems and networks.

Insurance

42 Is cybersecurity insurance available and commonly purchased?

Cybersecurity insurance is available in the United Kingdom from insurance providers such as ABI and Hiscox. A 2018 report (by Ovum and FICO) suggests that there has been a significant rise in the number of UK businesses with cybersecurity insurance. However, many UK businesses do not have full cover (for all cybersecurity risks) and arguably therefore do not have sufficient protection in the event of security breaches and data loss.

Right to be forgotten

43 Does your jurisdiction recognise or regulate the 'right to be forgotten'?

Yes, the 'right to be forgotten' is recognised in the United Kingdom. Following the CJEU decision in *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD)*, UK residents may apply to internet search engines with EU operations to remove search results that link to pages containing their personal data. Google has received a number of applications from UK citizens for deletion of links to pages containing their personal data. The ICO has sought to uphold individuals' rights where it has found that Google has mismanaged requests for the removal of information through discussion and negotiation, but also has enforcement powers available to it. In April 2018, Mr Justice Warby handed down the first two judgments relating to the 'right to be forgotten' in England and Wales: *NT 1 & NT 2 v Google LLC* [2018] EWHC 799 (QB). While the two cases came to opposite conclusions on the facts, the High Court followed the principles set out by the CJEU and concluded that the right to be forgotten is recognised in the United Kingdom. Although decisions of the High Court do not establish binding precedent, they can be persuasive and it is likely that the UK courts will continue to recognise the right to be forgotten.

Article 17 of the GDPR introduces a right for individuals to have their personal data erased by making a verbal or written request to a controller. The right is not absolute, only applying in certain circumstances set out in article 17(1), for example, where the data is no longer necessary for the purpose it was originally collected for, or where the data is being processed unlawfully.

The United Kingdom intends to transpose the GDPR into UK law when the United Kingdom exits the European Union, through the EUWA. In the event that the United Kingdom exits the European Union without a deal, the UK government has advised that data subjects in the United Kingdom will continue to benefit from the same high levels of data protection and that the same GDPR standards will continue to apply in the United Kingdom, including the right to be forgotten.

Email marketing

44 What regulations and guidance are there for email and other distance marketing?

The PECR places restrictions on how a website provider can carry out unsolicited direct marketing by email, which also apply to any message that consists of text (eg, short message service), voice, sound or images. Under the PECR, a website provider can only carry out unsolicited marketing (ie, marketing which has not specifically been asked for) by email if the individual being targeted has given his or her consent, except where the website provider has obtained the individual's details in the course of a sale or the negotiations for a sale of a product or service to that individual, the messages are only marketing similar products or services of the website provider, and the individual is given a simple opportunity to refuse the marketing when their details are collected and, if they do not opt out, the website provider gives the individual a simple way to do so in every future message. The opt-out option should allow the individual to reply directly to the message.

The 'consent' standard required for direct marketing is now that of the GDPR's consent requirements. For example, organisations cannot leave checkboxes opting a customer into direct marketing 'ticked' on

© Law Business Research 2019

the assumption that a customer can un-tick this box if he or she does not wish to receive this marketing. Much of the GDPR's consent requirements were already highlighted as 'best practice' within the ICO's guidance on direct marketing, so many organisations should already be considerate of most of the new requirements.

The ICO has recently published updated guidance on direct marking, which provides enhanced directions for organisations to comply with the rules and their obligations set out in the DPA and PECR. This includes emphasising that not-for-profit organisations are not exempt from the DPA or PECR and must ensure that their marketing activities are held to the same standards as any other organisation (including obtaining specific consent for e-marketing, screening calls using a telephone preference service and providing information to customers about when and where their personal information will be used).

Individuals are entitled to opt out of receiving marketing at any time and website providers must comply with any opt-out requests promptly. Marketing companies must provide details of their identity and a valid address to recipients of marketing material. The rules on email do not apply to emails sent to organisations except with regard to the rules as to identity and the provision of an address, although individuals' email addresses at an organisation will be subject to the DPA.

The updated guidance also provides that in situations where an organisation may wish to directly market to their customers with material relating to a third party, the organisation should have obtained the relevant consents from the customers to obtain such marketing material from the third party, even if the customer details always remain under the custody and control of the original organisation. With respect to unsolicited direct marketing by third parties by email, this should only be done with the data subject's explicit consent by way of an express opt-in.

The updated guidance stipulates that when using bought-in marketing lists, organisations should not rely on them if the list broker cannot provide details of when and how the consent was obtained.

Consumer rights

45 | What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

All individuals have:

- the right to prevent processing likely to cause damage or distress;
- the right to access personal data;
- the right to prevent direct marketing;
- the right in relation to automated decision-taking; and
- the right of rectification, blocking, erasure (right to be forgotten) and destruction of personal data.

Individuals also have the right to compensation in the event that individuals suffer material or non-material damage as a result of an infringement of the GDPR. The same rights apply to foreign individuals. There may be other remedies for failures to process personal data lawfully available through the common law.

TAXATION

Online sales

46 | Is the sale of online products subject to taxation?

The sale of online products by a UK website operator is generally viewed by the UK taxation authorities as the supply of a service that is subject to VAT, subject to certain thresholds being exceeded. This includes where sales are made from the United Kingdom to an EU consumer, and possibly to an EU business depending on whether the EU business is itself VAT registered in its home state when the supplier may be able to zero-rate VAT. Where a UK business's sales exceed a VAT threshold in a EU member state, the UK business may need to register for VAT in that member state.

With respect to downloads (again treated as services), whether VAT is payable will depend on whether a consideration is paid (in money or in kind) for a supply of services to take place. As digitised products are regarded as services, certain products that in hard copy form are zero-rated (eg, books) may be subject to VAT when supplied in digitised form.

In respect of certain classes of services provided electronically, a 'reverse charge' procedure operates which deems the place of supply to be where the recipient resides, rather than the location of the supplier. In such cases, the UK supplier would not have to account for VAT on sales to business customers within the European Union or outside it, but the EU customer would have to account for VAT in its member state. The aim of this provision is to ensure a level playing field for business-to-business transactions whether they take place with customers within the European Union or outside it.

These provisions also apply in respect of services supplied by a supplier outside the European Union, meaning that an EU business customer may have to account for VAT in its member state on such transactions. After the United Kingdom exits the European Union, these provisions will continue to apply where a UK company does business in an EU member state.

The position differs with regard to consumers where the supply will be treated as within the European Union if the recipient resides there. Supplies to UK recipients will therefore be subject to UK VAT regardless of where the supplier resides. The current regime permits non-EU based suppliers to register in the member state of their choice. No VAT is required to be accounted for on supplies to non-EU recipients.

As part of the EU Commission's digital single market strategy, an EU-wide digital services tax has been proposed. No agreement has been reached yet and it is unlikely that any significant progress will be made before the UK exits the European Union.

At the time of writing, nothing has been finalised with respect to Brexit; the ultimate position on taxation for online businesses operating in the United Kingdom and the European Union is therefore uncertain.

Server placement

47 | What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

A UK company placing its servers outside the United Kingdom may find itself subject to local tax laws of the country in which it has placed its servers if the laws of the country in question find such servers to constitute a permanent establishment that thereby creates a taxable presence. In certain countries, the carrying on of business through a website may constitute a permanent establishment for local-law purposes, making the UK company potentially liable to pay tax in that jurisdiction. Even if the servers of a UK tax resident placed outside the United Kingdom do not create a permanent establishment for the purposes of the jurisdiction in which the servers are placed, the UK company will still be liable for UK tax on income made through its e-commerce activities.

The UK government's current position is that neither the operation of a website itself nor the location of a server in the United Kingdom will constitute a permanent establishment in the United Kingdom. The UK's position in this regard is stated in the OECD's Committee on Fiscal Affair's report dated 22 December 2000 titled 'Clarification on the Application of the Permanent Establishment Definition in E-commerce: Changes to the Commentary on the Model Tax Convention on Article 5'. This is at odds with the views of other countries and it remains to

© Law Business Research 2019

be seen whether this position will be maintained. It should be noted, however, that a permanent establishment could nevertheless exist in the United Kingdom if other factors for the creation of such a permanent establishment are met and the position will be fact-specific in each case.

Company registration

48 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

In the United Kingdom, VAT applies to domestic internet sales. Companies making or intending to make taxable supplies of goods or services in the course of or furtherance of a business in the United Kingdom must be registered for VAT purposes if the taxable turnover exceeds or is expected to exceed specified limits.

Returns

49 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

In these circumstances, unless the goods are re-exported by the recipient, the recipient will not be able to reclaim any VAT and duty paid by the recipient. If the goods are returned to a high street branch of an offshore company, if the high street branch refunds any VAT and import duty paid by the recipient on the original supply by the offshore company, the high street entity may not be able to deduct the refunds for corporation tax purposes.

GAMBLING

Legality

50 Is it permissible to operate an online betting or gaming business from the jurisdiction?

The Gambling Act 2005 (the Gambling Act), which came into force in the United Kingdom in full from September 2007 and which repeals the Betting, Gaming and Lotteries Act 1963, the Gaming Act 1968 and the Lotteries and Amusements Act 1976, represents a radical shift in gambling law in the United Kingdom. The Gambling Act contains specific provisions regulating various technological means by which gambling activities can now be conducted. The Gambling Act adopts the concept of 'remote gambling' to cover gambling where the participants are not face-to-face on the same premises, and defines remote gambling to mean gambling where people are participating by means of remote communication, including the internet. Gambling is defined as including gaming and betting.

The Gambling Act establishes two comprehensive offences: providing facilities for gambling or using premises for gambling, in either case without the appropriate permission. Such permission may come from a licence, permit or registration granted pursuant to the Gambling Act or from an exemption given by the Gambling Act. Where authority to provide facilities for gambling is obtained under the Gambling Act, it will be subject to varying degrees of regulation, depending on the type of gambling, means by which it is conducted, and people by whom and to whom it is offered.

Persons operating remote gambling sites through the use of equipment situated in Great Britain must obtain a remote gambling licence, by virtue of section 36 of the Gambling Act, irrespective of whether the facilities are provided to people in or outside Great Britain. The Gambling (Licensing and Advertising) Act 2014 came into force on 14 May 2014 and requires all 'remote gambling operators' to obtain a Gambling Commission licence if they want to offer their services to British customers, regardless of the country in which the operator is based.

Section 5(2)(c) of the Gambling Act provides a general exception for entities such as ISPs (which do no more than act as information carriers) to the offence for providing facilities for gambling without a licence.

Subject to limited exceptions for gaming machines, section 41 makes it an offence to manufacture, supply, install or adapt computer software for remote gambling without an operating licence.

The Gambling Act also creates an offence where a person based in Great Britain uses remote gambling equipment to enable a person in a prohibited territory (to be designated by the relevant secretary of state) to participate in remote gambling.

The Gambling Act introduces a unified regulator for gambling in Great Britain, the Gambling Commission (the Commission), taking over from the Gaming Board for Great Britain, and a new licensing regime for commercial gambling (to be conducted by the Commission or by licensing authorities, depending on the matter to be licensed). The Gambling Act removes from licensing justices all responsibility for granting gaming and betting permissions, which they exercised previously. Instead, the Commission and licensing authorities will share between them responsibility for all matters previously regulated by licensing justices.

The Commission will not regulate spread betting, which is currently the preserve of the FCA. The Commission, in addition to assuming responsibility for regulating gaming, the National Lottery (following the abolition of the National Lottery Commission) and other certain lotteries, will take on responsibility for regulating betting. The Commission will be responsible for granting operating and personal licences for commercial gambling operators and personnel working in the industry.

The three objectives underpinning the functions of the Commission and licensing authorities in relation to gambling are:

- the protection of children and other vulnerable people at risk of being harmed or exploited by gambling;
- the prevention of gambling from being a source or support of crime or disorder; and
- ensuring that gambling is conducted in a fair and open way.

In respect of the National Lottery, the three objectives set out by the Commission are to ensure that:

- every lottery that forms part of the National Lottery is run with all due propriety;
- the interests of every participant are protected; and
- subject to the duties in the last two points, ensure that the proceeds of the National Lottery are as great as possible.

51 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Residents of the United Kingdom are permitted to use online casinos and betting websites. One of the key concerns of the Gambling Act is the protection of children and section 46 provides that a person will commit an offence if he or she invites, causes or permits a child (under 16) or a young person (under 18) to gamble. 'Inviting' includes advertising and other actions that bring attention to the facilities available for gambling. Section 63 provides a defence to the offence if the person can prove that all reasonable steps were taken to determine the individual's age and reasonably believed that the person in question was not a child or young person. Section 48 provides that, except in limited circumstances, it is an offence for a young person to gamble.

Section 64 enables the use of children and young persons in test purchasing operations for the purpose of assessing whether underage gambling laws are being complied with.

© Law Business Research 2019

OUTSOURCING

Key legal and tax issues

52 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

A provider of outsourcing services must ensure that the agreement provides for (as a minimum):

- the definition and scope of the services to be provided;
- the service levels being committed to;
- the potential remedies available for failure to meet such service levels and the agreement in general (including appropriate liability caps);
- change control provisions to properly deal with changes that may arise during the course of the agreement;
- dispute resolution procedures that are sufficiently flexible to enable small-scale disputes to be resolved quickly and informally;
- intellectual property ownership issues;
- imposing appropriate data protection obligations on the data processor;
- choice of law (particularly where the parties are in different jurisdictions); and
- exit management.

Employee rights

53 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, and do the rules apply to all employees within the jurisdiction?

The Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) came into force on 6 April 2006, replacing the 1981 Regulations of the same name. TUPE applies to all employers in the United Kingdom and cannot be contracted out of. TUPE is intended to protect employees by automatically transferring the employees and associated liabilities to a new employer if the business in which they are employed changes hands. TUPE will apply in most circumstances where an employer outsources or makes a 'service provision change' by engaging a third party to provide services that it previously provided in-house.

TUPE applies when a 'relevant transfer' occurs. A relevant transfer occurs on the transfer of an economic entity that retains its identity. In determining whether a relevant transfer has occurred, the courts will review a number of factors, for example, whether any customers are transferred with a service.

On a relevant transfer, TUPE provides that 'all the transferor's rights, powers, duties and liabilities under or in connection with the transferring employees' contracts of employment are transferred to the transferee'. This includes rights under the employment contract, statutory rights and continuity of employment and includes employees' rights to bring a claim against their employer, for example, for unfair dismissal, redundancy or discrimination. Employees that are transferring do so on their present terms and conditions and without affecting their present rights and liabilities. Except where the new employer can rely on a defence of economical, technical or organisational reason, any dismissals made by the new employer will be automatically unfair where the sole or principal reason for the dismissal is the transfer or a reason connected to the transfer, and the new employer is prohibited from making any changes to the terms and conditions of employment of the transferred employees if the sole or principal reason for the variation is connected to the transfer.

Incoming and outgoing employers have certain specific obligations with regard to employees on a business transfer and must inform and consult representatives of affected employees in sufficient time to enable proper consultation by the outgoing employer. In particular, changes or proposals for changes must be discussed. The incoming employer must supply sufficient information to the outgoing employer to enable the outgoing supplier to comply with its obligations to inform and consult. If the incoming and outgoing employers are found by an employment tribunal to have failed to inform and consult employees, it can award such compensation as it considers just and equitable up to a maximum of 13 weeks' pay per affected employee. Unless the transfer agreement provides otherwise, such liability can be split between the incoming and outgoing employers.

TUPE 2006 introduced a duty on the outgoing employer to provide the incoming employer, no less than 14 days before the transfer, with certain written information regarding the transferring employee (eg, particulars of employment) and details of the rights and liabilities that will transfer. Failure to comply with this duty can expose the outgoing employer to a claim for compensation by the incoming employer.

ONLINE PUBLISHING

Content liability

54 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability? Is it required or advised to post any notices in this regard?

Mistakes fall short of fraud or deliberate acts or omissions, and whether a publisher itself would be liable may depend on whether the publisher is publishing information on its own behalf or merely in the capacity of a platform provider.

Liability could potentially arise in a number of scenarios and could potentially result in a contractual claim (if a publisher has warranted the information as correct, for example, and loss arises) or a claim for defamation if the mistake related to a living individual. The most likely liability with respect to mistakes, however, is negligence and in particular negligent misstatement in circumstances where a 'special relationship' exists between the parties. For a special relationship to exist, there must be, most importantly, foreseeability of reliance by the representee, sufficient 'proximity' between the parties, and it must be just and reasonable for the law to impose the duty. This may be of concern where bespoke advice is provided on a website.

A publisher could potentially also be liable for negligent misrepresentation under the Misrepresentation Act 1967, where a mistake in information provided on a website induced a person to enter into a contract with the publisher. It could, however, be argued that a mistake falls short of the standard of negligence required to enable such a claim to proceed.

Subject to satisfying tests as to incorporation of a term limiting liability and reasonableness, liability for negligent misstatement and negligent misrepresentation could be limited (although probably not avoided altogether without risk of failing the reasonableness test) by website terms and conditions.

Databases

55 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

A database for English law purposes is a collection of independent works, data or other materials that are arranged in a systematic or methodical way and are individually accessible by electronic or other means. Such databases may be protected by copyright or a separate database right, each of which provides certain rights against unauthorised use and reproduction. According to the Copyright and Rights

© Law Business Research 2019

in Databases Regulations 1997 (as amended), for a database to enjoy copyright protection, the selection or arrangement of the database must amount to an intellectual creation of the author. Database rights may exist in a database where there has been a substantial investment in obtaining, verifying or presenting the contents of the database. Even where a database does not enjoy copyright protection or no database right exists, the website provider could potentially control use of the databases through its terms and conditions.

DISPUTE RESOLUTION

Venues

56 Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There are no specialist courts in the United Kingdom which deal specifically with online/digital issues and disputes.

ADR

57 What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

In the United Kingdom, as well as the traditional alternative dispute resolution (ADR) mechanisms of mediation and arbitration, it is possible to rely on ombudsman services, such as the Communications Ombudsman. The Ombudsman's role is to resolve disputes between consumers and companies that are signed up to the scheme. The Ombudsman has the power to require companies to take a variety of actions, including offering a financial reward to the consumer.

Two new ADR Regulations were introduced in the United Kingdom in 2015, implementing the EU ADR Directive. These regulations require most businesses which sell directly to consumers to direct the consumer to a certified ADR scheme. Currently, UK citizens can access the European Online Dispute Resolution (ODR) process that allows consumers to make a complaint against a trader where goods or services have been bought online. Traders in the European Union are obliged to provide a link to the ODR platform on their website. Following a no-deal Brexit, UK consumers will not be able to use ADR providers in the European Union and will not be able to use the ODR Platform. If there is a deal, consumer protections will remain in place during the implementation period.

UPDATE AND TRENDS

Key developments of the past year

58 Are there any emerging trends or hot topics in e-commerce regulation in the jurisdiction? Is there any pending legislation that is likely to have consequences for e-commerce and internet-related business?

The GDPR will force e-Commerce businesses to be more transparent about the way in which they process personal data as well as imposing on those businesses a need to be more innovative in the ways in which they obtain permission to market to and otherwise engage with consumers.

We are already seeing an increase in the creation of privacy preference centres whereby consumers are encouraged to be more in control of their own personal data, with the e-commerce business appearing to be more of an ethical custodian.

The increased enforcement and fines under the GDPR have raised data management practices to the same compliance level as other regulatory regimes such as anti-bribery and anti-trust.

BRISTOWS

Robert Bond
robert.bond@bristows.com

100 Victoria Embankment
London
EC4Y 0DH
United Kingdom
Tel: +44 20 7400 8000
www.bristows.com

The draft e-Privacy Regulation is already causing e-commerce businesses to revaluate legacy databases and to proactively re-permission personal data for both business to consumer as well as business-to-business relationships.

Both the GDPR and the draft e-Privacy Regulation are focusing attention on the real value of data as well as the unlawful processing of personal data.

Non-compliance with the law will not only lead to the risk of enforcement and fines but also the prospect of damage to reputation and brand and, even further, the likelihood of consumer class action claims for compensation when personal data is not managed nor protected in accordance with the law.

© Law Business Research 2019

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-138-4

© Law Business Research 2019