Digital Business in the UK (England and Wales): Overview

by Craig Giles and Will Deller*, *Bird & Bird LLP*

Country Q&A | Law stated as at 01-Mar-2022 | England, Wales

A Q&A guide to digital business in the UK (England and Wales).

The Q&A gives a high-level overview of matters relating to regulations and regulatory bodies for doing business online, setting up an online business, electronic contracts and signatures, data retention requirements, security of online transactions and personal data, licensing of domain names, jurisdiction and governing law, advertising, tax, liability for content online, insurance, and proposals for reform.

This resource may be affected by Brexit. Please note the law-stated date of the resource, and that it may not incorporate all recent developments. The UK left the EU on 31 January 2020. The transition period ended on 31 December 2020 (see *Brexit essentials: Q&As on agreements and operation of UK law: What happened at the end of the transition period?*). This Country Q&A will be updated in line with our usual publication schedule following the end of transition (see *Guide to assessing legal change after end of post-Brexit transition period* and *UK law after end of post-Brexit transition period: overview*). If you require more specific information, please see *Beyond Brexit: the legal implications*.

Regulatory Overview

1. What regulations apply for doing business online (for business-to-business and business-to-consumer)?

English law governing the conduct of business online is set out in a number of different statutory instruments. This area of law has been subject to increasing harmonisation at EU level, although following the UK withdrawal from the EU there may be greater disparities between the two sets of laws in the future.

The following regulations are of particular significance:

- The E-Commerce Regulations 2002 (E-Commerce Regulations) impose a range of obligations on the operators of commercial websites, in particular obligations to provide users with certain information about the operator and its services.
- The Consumer Rights Act 2015 (CRA) has consolidated a range of previous UK consumer rights legislation and updated certain areas, including statutory implied terms in consumer contracts and the remedies for breach available to the consumer.
- The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (Consumer Contract Regulations) place additional obligations on website operators who deal with consumers as well as introducing cancellation rights for consumers.
- The Consumer Protection From Unfair Trading Regulations 2008 (CPRs) prohibit various unfair practices by traders, such as misleading actions or omissions, and include a "blacklist" of prohibited commercial practices.
- The Provision of Services Regulations 2009 (POS Regulations) provide that in the provision of services, traders must make specified information available to customers and meet certain standards when handling complaints.
- The UK GDPR (that is, the General Data Protection Regulation GDPR (*(EU) 2016/679*) provisions as implemented into UK law by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419)) and Data Protection Act 2018 (DPA) contain provisions around the use of personal data, including concerning website users.

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations) govern direct marketing (both solicited and unsolicited) by means of electronic communication.
- The Online Intermediation Services for Business Users (Enforcement) Regulations 2020 (P2B Regulations) impose obligations on providers of online platforms or search engines that are used by businesses to reach consumers.

2. What legislative bodies are responsible for passing legislation in this area? What regulatory and industry bodies are responsible for passing regulations and codes in this area?

Major UK legislation must be passed as an Act of Parliament. Additionally, Acts of Parliament often empower certain government ministers to make further, more detailed regulations in specific areas (for example, the Department of Business, Innovation and Skills oversees subordinate legislation for online services and consumer protection).

There are several national bodies that issue codes of conduct and guidance which do not have the force of law but can either influence interpretation of the law or bind companies that have agreed to comply with self-regulatory systems. By way of example:

- The Information Commissioner's Office (ICO) is the independent regulatory body which oversees compliance with the:
  - UK GDPR;
  - DPA; and
  - PEC Regulations.
- The Committee of Advertising Practice (CAP) publishes codes which govern broadcast and non-broadcast (including online) advertising in the UK. The CAP Codes are enforced by the Advertising Standards Agency (ASA). See *Question 32*.

Setting up a Business Online

3. What steps must a company take to set up an existing/new business online?

New businesses should establish a vehicle through which the business will operate (for example, a limited liability company). The business should be registered at Companies House, with HMRC and with the ICO (unless an exemption applies). Before

choosing a company name or trading name, the owners should check that there are no existing companies trading with the same or a similar name which may cause confusion or potential issues with intellectual property infringement (see *Question 28*).

The business will need to establish an online trading presence and acquire a domain name. Unless the business already has staff with the necessary expertise, it will need to engage a third party to design and develop the website and an internet service provider to host the website. The company's website must provide certain information to users (see *Question 39*). This is frequently provided in an "About Us" or "Terms of Use" section and in a privacy policy and cookies policy. Consent will be required for any cookies other than those which are non-essential, and should be collected on the website landing page by way of a cookie banner (see *Question 18*). If the business intends to trade through the website, it will require separate terms of sale/service.

In addition to the general legislation affecting online trade, the business owners should also check whether there are any rules and regulations specific to the type of business they intend to run.

4.What types of parties can an online business expect to contract with?

Depending on the nature of the business, the following agreements are usually required:

- Website development: this should set out the company's functional and visual specification for the website, maintenance and support obligations, and the ownership of intellectual property rights (for example, in the design of the web pages and underlying software).
- Website hosting: this should detail the scope of the services (for example, whether security, maintenance or support is provided), the specification of the server, and minimum availability requirements.
- Content licences: where the business does not own all content that will be displayed on the site it must ensure its licences with third parties are appropriate (for example, covering how the content is to be used, the territorial scope and the term of the licence).
- Agreements with users: terms setting out the basis on which users can access the site, a privacy and cookies policy and (where applicable) terms of sale/service.

5. Is there any law or guidance that might affect the design of the website or app (for example, relating to access by disabled people or children)?

Website Accessibility

People with the protected characteristics set out in section 4 of the Equality Act 2010 should not be discriminated against when using a service (*Equality Act 2010*). Providers of information society services must make "reasonable adjustments" to ensure

that their services are accessible to disabled people, and are designed to meet the needs of people with protected characteristics (including disabled people) so that they can, as far as possible, receive the same standard of service.

The governing statutory body (that is, the Equality and Human Rights Commission) has published a *code of practice* to help organisations understand how to discharge these obligations (see *Equality and Human Rights Commission: Services, Public functions and Associations: Statutory Code of Practice*). Additionally, the World Wide Web Consortium has published *website accessibility guidelines*, which provide an indication of the standard the courts would reasonably expect (see *W3C Web Accessibility Initiative: WCAG 2 Overview*). Public sector organisations are expected to meet the *WCAG 2.1 AA accessibility standard* (unless they are exempt) (*Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018*).

Children's Access to Websites

The ICO's Age Appropriate Design Code applies to providers of information society services likely to be accessed by children in the UK. The Code sets a number of enhanced privacy standards for the processing of children's data, including requirements to:

- Ensure privacy notices are appropriate to the age groups accessing the service.
- Conduct a data protection impact assessment.
- Set processing for non-core activities including profiling to "off" by default.

There is also a prohibition on data sharing unless there is a compelling reason to share.

The Code came into force on 2 September 2020 with a 12-month transition period. While the Code itself isn't law, the ICO has made it clear that organisations who fail to comply with the Code will find it difficult to demonstrate that their processing is fair, which will give rise to a breach of UK GDPR and will be enforced in line with the ICO's Regulatory Action Policy. (For further detail on the Age Appropriate Design Code, see below).

When embarking on a new project which uses personal data, organisations must evaluate whether the processing of personal data for the website or the app is likely to result in high risk to the affected individuals. If so, a Data Protection Impact Assessment (*Article 35 UK GDPR*) must be carried out. This process may involve prior consultation with the ICO. The ICO has produced guidance on conducting DPIAs including triggers for consultation.

Other guidance likely to be of particular relevance to those building websites and apps are:

- The ICO's guidance on the use of cookies and similar technologies.
- The ICO's direct marketing guidance (which will soon be replaced by a direct marketing code of practice.

6. What are the procedures for developing and distributing an app?

Where the business enters into an agreement with an app developer, the terms must address what licences will be needed to develop and distribute the app, including for example, content and software licences (and address intellectual property rights and ownership in any newly created or modified content or software). The agreement should also specify the required functionality of the app, development milestones and testing phases, and any ongoing support obligations of the developer.

If the business wants to distribute the finished app through an app store, it will usually enter into a distribution agreement with the app store provider. The agreements of the largest providers (Apple, Google and Microsoft) are publicly available on their websites. Businesses frequently require users to enter into an End User Licence Agreement (EULA), which provides the terms and conditions applicable to the use of the app. These may include data protection terms as well as certain mandatory terms stipulated by the relevant app store provider. The user must be provided with a copy of the EULA and must accept it before the user can download and use the app. The user must also be presented with relevant privacy information (see *Question 16*) and be given a mechanism through which the user can consent (or withhold consent) to non-essential cookies and similar technologies (see *Question 18*). If the business wishes to accept payments through the app, an agreement with a third-party payment services provider can also be required**.**

Running a Business Online

Electronic Contracts

7. Is it possible to form a contract electronically? Are there any limitations?

Requirements

For an online contract to be binding there must be an offer, acceptance, an intention to create legal relations, and certainty of terms.

Offer and Acceptance

To give the trader control over the terms of the contract, a website's terms and conditions often:

- State that by submitting an order the customer is making an offer.
- Describe when the trader is deemed to have accepted that offer, for example, once it has issued an order confirmation e-mail, or dispatched the goods.

Incorporation of Terms

The terms of the contract must be brought to the attention of the customer before the contract is completed. The English courts have not given definitive guidance as to how online terms and conditions must be incorporated, but the most effective way is to design the website so that the customer is unable to complete their order until they have scrolled down the full terms and

conditions on-screen and clicked an "I accept" button (or similar). This is known as a click-wrap contract. In the context of software licence agreements (known as end user licence agreements) there are two other common forms of contract:

- Browse-wrap contracts, where a user is notified that by continuing to use the software they are bound by certain terms and conditions, but without the user having to take a positive action to accept them.
- Shrink-wrap contracts, where a user purchases a physical software product and the terms are either included with the packaging or in a file that must be opened during installation.

Business-to-Consumer (B2C) Context

In a B2C context, the Explanatory Notes to the Consumer Rights Act 2015 (CRA) reference the Law Commission and Scottish Law Commission's joint guidance note on unfair terms (see, in particular, Appendix C). The Explanatory Notes state that browse-wrap contracts are unlikely to be deemed contracts, and therefore capable of placing contractual obligations on a consumer, as there is no valid acceptance (as there is with a click-wrap contract).

Shrink-wrap contracts are also unlikely to be enforceable against consumers on the basis that they are likely to be unfair. Schedule 2 to the CRA sets out a list of terms which may be considered unfair in consumer contracts. These include a term which has the object or effect of irrevocably binding the consumer to terms with which the consumer has had no real opportunity of becoming acquainted before the conclusion of the contract. However, both types of contract may potentially be considered a "non-contractual notice", so a form of warning to the consumer that may (for example) serve to discharge a duty of care that the website operator may otherwise have faced, and can serve to grant a unilateral licence to use the applicable software. Even as non-contractual notices, both browse-wrap and shrink-wrap contracts must comply with Part 2 of the CRA (unfair terms).

Business-to-Business (B2B) Context

In a B2B context, it is unlikely that a browse-wrap contract would be legally binding, as there is no opportunity for the user to accept the terms.

The position on shrink-wrap contracts is unclear. While the terms may state that by downloading the software the user agrees to be bound by the terms of the licence, the user is still not made aware of those terms at the time of concluding the contract. The Scottish Court of Session held that a shrink-wrap licence was enforceable in a case where a software package stated that opening the package indicated acceptance of the terms and conditions, and that the purchaser was entitled to return the packaged software up until the moment that the purchaser opened the package (*Beta Computers (Europe) Ltd v Adobe Systems (Europe) Ltd, 14 December 1995*). However, in the absence of English case law on this matter, the legal foundation for this well-established business practice remains unclear under English law.

Regulatory Requirements

Where orders are placed online, the E-Commerce Regulations require the trader to provide certain specific information, including:

- The different technical steps to follow to conclude the contract.
- The languages offered for the conclusion of the contract.

The trader should also provide terms and conditions in a way that allows the customer to store and reproduce them (*Regulation 9*).

The customer must be given the opportunity to review and correct input errors before completing the purchase. The trader must acknowledge receipt of the order by electronic means without undue delay, for example, by sending an order confirmation e-mail (*Regulation 11*). Businesses, but not consumers, can agree to contract out of these provisions.

Consumer Contracts

Traders must provide consumers with additional specific information before entering into any contract, for example, the main characteristics and total costs of the relevant products/services, the arrangements for payment and delivery, and the existence of any right to cancel (*Regulation 13 and Schedule 2, Consumer Contract Regulations*). Where orders are placed online, the trader must clearly label the order button to indicate that placing the order entails an obligation to pay the trader by using words such as "order with obligation to pay" (*Regulation 14, Consumer Contract Regulations*). The trader must give the consumer confirmation of the contract, including the pre-contract information, in a "durable medium" within a reasonable period, and no later than delivery of the goods or commencement of the services (*Regulation 16, Consumer Contract Regulations*). The Consumer Rights (Payment Surcharges) Regulations 2012 (SI 2012/3110) (as amended) further provide that a trader cannot impose any surcharges on consumers when making an online payment using credit or debit cards and similar online payment services (for example, PayPal).

Limitations

In September 2019, the Law Commission published a report confirming that electronic signatures may be used to execute documents, including deeds (see *Question 13*).

It is crucial that the execution formalities are still satisfied, such as the requirement for a witness, if applicable. Some products by their nature require additional safeguards when being bought and sold by means of an electronic contract formed at a distance (see *Question 32*).

In general, contracts do not need to be available in a certain language (such as English) to be enforceable. However, contracts with consumers are subject to a transparency requirement, which requires that the terms are legible and are written in plain and intelligible language (*section 68, CRA*). Terms made available in another language are unlikely to satisfy the transparency requirement for UK-based consumers.

8. What laws govern contracting on the internet?

B2B Contracts

Businesses must comply with the E-Commerce Regulations, including the information requirements (see *Question 7 and Question 39*). Other statutory provisions such as the Sale of Goods Act 1979, the Supply of Goods and Services Act 1982 and the Unfair Contracts Terms Act 1977 (UCTA), apply to contracts formed online as they would do to a contract formed by other means.

The P2B Regulations impose obligations on providers of online platforms and search engines used by businesses to reach consumers, including:

- To provide certain information in terms and conditions.
- To operate a complaints handling procedure.
- Minimum notice requirements for termination, suspension or restriction of business users' accounts.

There are also legal requirements where the contract involves the transfer of personal data between parties:

- The UK GDPR provides for requirements between controllers and processors (*Article 28, UK GDPR*).
- The UK GDPR requires that an agreement is in place where there are joint controllers of data (*Article 26, UK GDPR*).
- The ICO's data sharing code of practice provides additional guidance on sharing personal data.
- Where the contract requires data to be transferred internationally, a lawful basis of transfer must be in place (*Chapter V, UK GDPR*).

Consumer Contracts

A business selling to consumers online must comply with the regulations applicable to B2B contracts (which generally cannot be contracted out of when dealing with consumers) and with additional consumer-specific regulation, in particular the Consumer Rights Act 2015 (CRA) and the Consumer Contract Regulations.

The CRA applies to contracts formed on or after 1 October 2015, and consolidates and updates a number of other pieces of consumer rights legislation. It incorporates a number of implied terms into consumer contracts (such as fitness for purpose and satisfactory quality), sets out a set of tiered remedies for consumers where their consumer rights are breached and grants statutory protection for consumers against unfair terms.

The Consumer Contract Regulations address what pre-contract information must be provided to consumers, including if contracting online, and the rights of consumers to a cooling off period within which they may cancel their contract and receive a refund with or without cause.

For more details on both pieces of legislation, see *Practice Note, Consumer law: introduction to key legislation*, and for information on the CRA generally, see *Toolkit, Consumer Rights Act 2015*.

EU Digital Single Market

EU legislation affecting online businesses that target customers in the EU include:

- The Unjustified Geo-blocking Regulation (*(EU) 2018/302*). This prohibits traders from discriminating on the basis of nationality, country of residence or establishment between potential online customers of goods and services.
- The Portability Regulation (*(EU) 2017/1128*). This places a requirement on providers of portable online content services to ensure consumers can access services obtained in their member state of residence while temporarily visiting other EU member states.

These measures ceased to apply in the UK at the end of the Brexit transition period, but are still relevant to businesses targeting customers in the EU.

Laws of Other Territories

If the trader intends to trade with customers from other countries, they must establish which country's governing law will apply to the contract. When targeting consumers from another country, the trader should be aware that those consumers may be entitled to the benefit of certain mandatory laws from their own territory.

9. Are there any data retention requirements in relation to personal data collected and processed through electronic contracting?

The trader must notify the customer whether the concluded contract will be filed by the trader and whether it will be accessible (*Regulation 9(1), E-Commerce Regulations*). Business customers, but not individual consumers, can contract out of this requirement.

Additionally, the UK GDPR imposes a general duty to retain personal data only for so long as is necessary, having regard to the purpose for which the data is collected or held (for example, for the purpose of fulfilling an order, or responding to a potential complaint or dispute).

10. Are there any trusted site accreditations available to confirm that the website has complied with minimum cybersecurity standards?

There are no official government trusted site accreditations for websites, although some accreditations may be of interest to website providers, such as:

- ISO 27001 is the international standard for information security management (which can be obtained through the British Standards Institution).
- Prominent private companies offering e-commerce accreditation schemes include Symantec, Paypal, and Norton.
- tScheme Limited operates an industry-led, self-regulatory system set up to approve electronic trust services, including qualified certificate services (see *Question 12*).

11. What remedies are available for breach of an electronic contract?

Remedies available for breach of an electronic contract are largely the same as those available for breach of any other type of contract.

Where a specific regulatory requirement is breached, additional remedies may be available. For example:

- A breach of the obligation in the E-Commerce Regulations to give the customer an opportunity to correct input errors could give the customer a right to rescind the contract.
- Traders who supply digital content online should note the additional requirements and remedies available under the Consumer Rights Act 2015 and the Consumer Contracts Regulations (see *Question 8*).
- In a B2C context, a breach of the obligation to provide the cancellation right in the Customer Contracts Regulations will extend the period in which the consumer can exercise that right.
- The GDPR provides for individual data protection rights which the individual may choose to exercise at any time. A breach of contract may prompt an individual to exercise these rights. Individuals also have the right to complain to the ICO, which may trigger an investigation. The ICO powers of enforcement include:
    - orders to cease certain processing activities or certain personal data; and
    - monetary penalty of GBP17.5 million or 4% annual worldwide turnover, whichever is higher (*S157(5), DPA*).

If the breach relates to the PEC Regulations, the ICO can issue a monetary penalty of up to GBP500,000.

E-Signatures

12. Does the law recognise e-signatures or digital signatures?

E-signatures are recognised under English law.

Applicable Legislation and Use

The legal framework is based on the Electronic Identification Regulation (*(EU) 910/2014*) (eIDAS), which came into effect on 1 July 2016 and was implemented by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016. eIDAS is an attempt to increase the use of electronic identification and authentication facilities and expand the legal framework governing electronic identification/documentation.

The UK regulations have been amended following the end of the Brexit transition period by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/89), largely to remove redundant provisions relating to intra-EU reciprocal arrangements.

Definition of E-Signatures/Digital Signatures

eIDAS defines an electronic signature as data in an electronic form that is attached to or logically associated with other data in an electronic form and used by the signatory to sign.

eIDAS also provides a definition of qualified electronic signatures. These are electronic signatures based on a qualified certificate and created by a secure-signature-creation device. Under eIDAS, these signatures satisfy the legal requirements of a signature in the same manner as a handwritten signature, and are admissible as evidence in legal proceedings.

tScheme Limited operates a voluntary accreditation scheme of certification services, and maintains a list of providers it has certified.

Format of E-Signatures/Digital Signatures

English law takes a broad view of what constitutes a valid electronic signature. According to the Law Commission, it is simply necessary that the signatory's activity indicates an intention to authenticate. Law Commission guidance on the topic gives the following non-exhaustive examples:

- Digital signature through use of an encryption system involving a certification authority (a type of advanced electronic signature).
- A scanned manuscript signature or a digitised version of a manuscript signature.
- The typing of a name.
- Clicking on an appropriately labelled button on a website (for example, "I accept").

For detailed guidance from the Law Commission, see *The Law Society: Execution of a document using an electronic signature*. This is guidance only and does not have legal effect.

COVID-19

HMRC is accepting e-signatures for stamp duty purposes while COVID-19 measures are in place. This change will be reversed once COVID-19 measures are lifted (check *HM Revenue & Customs: Pay Stamp Duty on shares* for updates).

The Law Society has released updated guidance on the use of e-signatures during the pandemic (*see The Law Society: Our position on the use of virtual execution and e-signature during the coronavirus (COVID-19) pandemic*). This is guidance only and does not have legal effect.

13. Are there any limitations on the use of e-signatures or digital signatures?

The practicalities of having the signature witnessed can make electronic execution of a deed impractical. In September 2019, the Law Commission published their "Electronic execution of documents" report (Report) to address uncertainty as to the formalities around the electronic execution of documents, particularly deeds.

The Report confirmed that electronic signatures are capable of executing documents, including deeds, provided that the signatory intends to authenticate the document and the execution formalities are satisfied. The Report took the view that the witnessing of a deed requires the physical presence of the witness (so this cannot be done remotely or by video link).

More generally, it can be harder to prove the validity of electronic signatures in comparison with handwritten signatures (where it is possible to use the evidence of a forensic handwriting expert). This risk can be mitigated to an extent through the use of a "qualified electronic signature" (*see Question 12*).

Implications of Running a Business Online

Data Protection

14. Are there any laws regulating the collection or use of personal data? To whom do the data protection laws apply?

The collection and use of personal data is regulated by the UK GDPR and the DPA. The UK GDPR and DPA apply to both data controllers (that is, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (*Article 4(7), UK GDPR)*) and to data processors (that is, the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (*Article 4(8), UK GDPR*), such as cloud service providers). The UK GDPR and DPA should be read in conjunction.

The EU GDPR was directly applicable in the UK up to the end of the Brexit transition period. The GDPR's provisions were implemented into UK law from the end of the transition period, with technical amendments being made to ensure that they work in a UK context, by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

Under the terms of the Withdrawal Agreement (in particular, Article 71), personal data relating to EU data subjects that was lawfully processed in the UK before the end of the transition period and continues to be processed in the UK by virtue of the Withdrawal Agreement, is subject to European Data protection law as it existed on 31 December 2020 (also known as "frozen GDPR"). Should the UK receive a positive adequacy decision from the European Commission it is likely that this element of regulation will fall away. The EU GDPR may still apply to the processing of personal data by UK-based organisations, where the EU GDPR's provisions on territorial scope are engaged.

15. How does the law define personal data or personal information?

The UK GDPR regulates personal data, defined in Article 4(1) of the UK GDPR. It does not regulate information relating to corporate bodies.

Personal data is defined as any information relating to an identified or identifiable natural person. An "identifiable" natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. "Identifiers" include online identifiers (*Article 4(1), UK GDPR*) provided by devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags (*Recital 30*).

The definition requires the data to relate to a "natural" person. Information about a "legal" person with a separate legal identity from its owners (such as a limited company) does not amount to personal data, although information relating to natural persons within the business (for example, employees and directors) may be personal data. Additionally, information relating to businesses operating without a separate identity from their owners (such as sole trader businesses) may be personal data (if the other elements of the definition are satisfied).

For more see *Practice Note: Overview of UK GDPR: Definitions: Personal data*.

16. Are there any limitations on collecting, storing or using personal data?

Fair and Lawful Data Collection

The UK GDPR restricts the collection and use of personal data. The UK GDPR requires data controllers to identify the appropriate "lawful basis" for each type of data processing that they perform (*Article 6, UK GDPR*). The UK GDPR generally permits the collection and use of personal data to the extent necessary for the performance of a contract with data subjects, or for taking steps at the request of the data subject with a view to entering into a contract. See *Practice Note, Overview of UK GDPR: First data protection principle: lawfulness, fairness and transparency*.

In most cases, personal data should not be collected by or on behalf of a data controller unless prescribed privacy information is provided to the data subject (*Articles 12 to 14, UK GDPR*). This information includes, among other things:

- Information about the types of personal data collected.
- The purposes for which the data will be used.
- The legal basis relied on to process the data.

For digital business, this requirement is usually addressed by the publication of a privacy notice. See *Practice Note, Overview of UK GDPR: Fair processing: information notices*.

Data Quality

The UK GDPR also imposes obligations on data controllers in relation to the quality of the personal data they collect and use, and the period for which they hold the personal data (*Article 5(1), UK GDPR*) (*see Practice Note, Overview of UK GDPR: Second data protection principle: purpose limitation*). Additionally, the UK GDPR "accountability" principle requires data controllers to be able to actively demonstrate compliance with the data protection principles (*Article 5(2), UK GDPR*) (*see Practice Note, Overview of UK GDPR: Accountability*).

Outsourcing Solutions

The UK GDPR does not expressly restrict cloud storage of personal data, but its provisions should be taken into account when cloud solutions are used by data controllers to store information that includes personal data. Data controllers retain legal responsibility for the security and integrity of data stored by or on their behalf on the cloud. They must ensure that any commercial agreement with third party cloud providers includes prescribed data protection provisions (*Article 28, UK GDPR*), and they are expected to monitor the cloud provider's compliance with these terms. See *Practice Note, Overview of UK GDPR: Processors*.

Storage of Personal Data Outside the UK

The UK GDPR restricts storage or transfer of personal data outside the EEA (through the use of cloud solutions or otherwise). Transfers of personal data from the UK are prohibited unless there is adequate protection for personal privacy (*Articles 44 to 50, UK GDPR*). See *Practice Note, Overview of UK GDPR: Transfers under UK adequacy regulations*.

For transfers to countries or organisations which do not benefit from an adequacy finding, a range of mechanisms can be relied on to deliver adequate protection, including the use of approved standard contractual clauses or the use of approved Binding Corporate Rules. See *Practice Note, Overview of UK GDPR: UK Binding corporate rules*.

The UK GDPR also permits transfers of personal data on the basis of certain derogations, in the absence of an adequacy decision or transfer mechanism (*Article 49, UK GDPR*). These derogations include contractual necessity and legitimate interests (applicable in limited circumstances) and each individual's explicit consent (although this has a higher validity threshold than the usual consent required under the UK GDPR). The UK GDPR has also made provision for the development of new data transfer mechanisms, for example, the use of approved codes of conduct or approved certification mechanisms (*Article 428, UK GDPR*), although none have yet been implemented.

Receiving Personal Data From the EEA

Since the end of the transition period, in the absence of a relevant adequacy decision from the European Commission, the UK is a "third country" for the purposes of transfers of personal data from the EEA. This means that a transfer mechanism or derogation (*see above*) will need to apply to transfers of personal data from the EEA to a UK-based recipient.

Rights of Data Subjects

Data controllers must recognise the rights of data subjects, which can impact on the ability of businesses, in certain circumstances, to retain and use personal data in the face of requests by data subjects to do otherwise. Digital businesses must ensure that systems used to store personal data are capable of accommodating the exercise of these new rights. See *Practice Note, Overview of UK GDPR: Rights of the data subject*.

17. Can government bodies access or compel disclosure of personal data in certain circumstances?

A significant number of public authorities and regulators have powers to access or compel disclosure of information that is relevant to the exercise of their regulatory functions, such as:

- The Information Commissioner has powers to require a data controller or data processor to provide specified information for the purpose of the Information Commissioner's tasks (for example, an audit). The Information Commissioner can only require such information by written information notice and the information to be provided in response does not extend to legally privileged information, or information that can expose the subject to risk of prosecution for an offence (other than an offence under the DPA or certain perjury laws).
- The Department of Work and Pensions has powers to compel specified organisations, including banks, insurers and certain utilities providers, to supply information for the purpose of preventing or detecting fraud.
- The Investigatory Powers Act 2016 (IPA) contains a variety of powers for the obtaining of customer communications information from telecommunications providers. See *Practice Note, Investigatory Powers Act 2016: overview*.

Privacy Protection

18. Are there any laws regulating the use of cookies, other tracking technologies like digital fingerprinting, or online behavioural advertising?

The use of cookies and similar technologies (referred to collectively as "cookies") is currently regulated by the PEC Regulations. Website operators cannot store information or gain access to information stored in the terminal equipment of a user unless the user is provided with clear and comprehensive information about the purpose of such storage or access and has consented to it (*Regulation 6*). However, Regulation 6 does not apply to cookies that are strictly necessary to provide an online service requested by the user.

Where user consent is required, it must satisfy the validity criteria established under the UK GDPR, so it must be a freely given, specific, informed and unambiguous indication of the data subject's agreement (by statement or a clear affirmative action) *(Article 4(11), UK GDPR*).

Additional requirements apply to the consent under Article 7 UK of the GDPR. For information on these and more, see *Practice Note, Cookies: UK issues and the impact of UK GDPR and DPA 2018*.

Where use of cookies involves processing of personal data, the provisions of the UK GDPR also apply.

Cybersecurity

19. What measures must contracting companies or internet providers take to guarantee internet transactions' security?

The PEC Regulations impose obligations on internet service providers to take appropriate technical and organisational measures to safeguard the security of the services they supply. As a minimum, this means that internet providers must:

- Ensure personal data can be accessed only by authorised personnel for legally authorised purposes.
- Protect the personal data they store or transmit against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage, processing, access or disclosure.
- Ensure the implementation of a security policy for the processing of personal data.

The collection of any such information is conditional on the deployment of technical and organisational measures as set out in Article 32 of the UK GDPR. See *Practice Note, Overview of UK GDPR: Data security and personal data breaches*. These measures might include:

- Pseudonymisation and encryption of personal data.
- The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.

Online businesses must comply with their own obligations under the UK GDPR to take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage, and will be similarly required to comply with their obligations under the UK GDPR (*Article 32, GDPR*).

To the extent that traders accept card payments from customers, they must ensure that their systems comply with the Payment Card Industry Data Security Standards (PCI-DSS), which stipulate how traders deal with customer information. Sensitive card authentication data must never be stored by the trader after authorisation of a payment transaction even if it is encrypted.

20. Is the use of encryption required or prohibited in any circumstances?

Neither the UK GDPR nor the PEC Regulations mandate the use of encryption. However, the UK GDPR obliges controllers and processors to implement appropriate measures to ensure a level of security appropriate to the risk (see *Question 19*). The types of measures envisaged by the UK GDPR which may be appropriate include pseudonymisation and encryption of personal data (*Article 32(1)(a), UK GDPR*). In many cases data encryption will be considered an appropriate and necessary measure

for the protection of personal data stored on mobile digital media, sensitive or confidential e-mail communications, and data held in the cloud.

Although the use of encryption by online businesses is not prohibited, under section 49 of the Regulation of Investigatory Powers Act 2000 (RIPA), law enforcement authorities have some powers to require decryption of a particular document or (in limited circumstances) to compel the disclosure of an encryption key by giving notice.

In addition, the Investigatory Powers Act 2016 (IPA) extends the previous power under RIPA to mandate a permanent interception capability. The IPA confers power on the Secretary of State to oblige telecommunications operators (defined broadly) to install permanent interception capabilities. The IPA also confers powers on government bodies to obtain warrants which may require the supply of information in intelligible form to the extent reasonably practicable. See *Practice Note, Investigatory Powers Act 2016: overview*.

21. Are electronic payments regulated?

The provision of payment services is subject to a complex set of regulatory requirements and involves a number of regulators.

The Payment Services Directive ((*EU) 2015/2366*) (PSD2), implemented in the UK by the Payment Services Regulations 2017 (PSRs), governs the provision of payment services in the UK by regulated payment service providers. The PSRs contains strict requirements on the conduct of business by print service providers, security and protection of customer data and strong customer authentication. See *Practice Note, Understanding the Payment Services Regulations 2017*.

Traders are generally free to accept electronic payments, subject to certain security requirements (see *Question 19*).

Some traders also use recurrent electronic payments in the form of direct debit transactions using an instruction to the consumer's bank or electronic money institution. These payments are subject to the banking industry consumer protection rules including the Direct Debit Guarantee vetting process.

Subscription pricing models are also becoming increasingly prevalent for electronic payments. Subscription terms and conditions are governed by contract and consumer protection laws (such as the Unfair Contract Terms Act 1977) and the payments model has been subject to increasing scrutiny by the Competition and Markets Authority.

22. Do any specific rules or guidance apply to websites aimed at (or that might be accessed by) children?

Contracts with individuals are generally only enforceable if the individual has reached the age of 18 (*section 1, Family Law Reform Act 1969*). Contracts with very young children are generally void. However, there are some circumstances in which contracts with older minors may be enforceable, including contracts for:

- "Necessaries" (for example, food and clothes).
- Education, apprenticeship and service (including employment).

Section 5 of the CAP Code (see *Question 32*) provides a series of restrictions on advertising to minors (including online).

Data Protection

The UK GDPR imposes specific obligations on website providers offering online services to children. See *Practice Note, Overview of UK GDPR: Children and consent*.

Data Protection Notices

Website providers must supply extensive information to data subjects about the data processing operations conducted (*Article 13, UK GDPR*) (see *Question 16*).

This information must be communicated in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (*Article 12(1), UK GDPR*).

Consent to Data Processing

Where online services are offered or supplied to a child and there is requirement under the UK GDPR to obtain consent to process the child's personal data, then parental consent or authorisation is required (*Article 8, UK GDPR*). The UK GDPR makes clear that children under the age of 13 can never themselves give consent to the processing of their personal data in relation to online services. Therefore, if an organisation seeks consent to process the personal data of a child under 13 in connection with the provision of an online service, parental consent or parental authorisation of consent is required. Website providers are expected to make "reasonable efforts" to verify that parental consent is given or that consent is authorised by a parent, in light of available technology.

Right to Erasure

The UK GDPR confers a right on all data subjects to obtain the erasure of their personal data where at least one of the grounds set out at Article 17(1) of the UK GDPR applies. One of the grounds on which this right can be exercised is that the personal data were collected in relation to the offer of online services to a child in circumstances where consent was given by or on behalf of the child. See *Practice Note, Overview of UK GDPR: The right to erasure and the right to be forgotten*.

Age Appropriate Design Code

The ICO has published its Age Appropriate Design Code (under section 123 of the DPA), which came into force on 2 September 2021 and applies to all providers of information society services likely to be accessed by children. The Code contains 15 standards that aim to provide children with "high privacy by default" and to automatically provide children with a built-in baseline of data protection whenever they access services online or through connected devices. For details of these standards, see *ICO: Age appropriate design: a code of practice for online services*.

23. Are there any laws protecting companies within your jurisdiction that resell or market online digital content, services or software licences provided by a supplier outside the jurisdiction?

The Commercial Agents (Council Directive) Regulations 1993 (SI 1993/3053), implementing Directive 86/653/EEC (Commercial Agents Regulations) govern the relationship between an agent and principal when an agent sells or purchases goods on behalf of its principal. The Commercial Agents Regulations contain some important protections protecting the agent's rights to commission. They do not extend to services or to other types of relationship that fall outside an agency (such as distributors).

In the UK, the courts have traditionally taken the view that the supply of software on a tangible medium (such as a CD) falls within the definition of "goods", whereas the electronic supply of software falls outside that definition. However, following a reference from the Supreme Court in *The Software Incubator Ltd v Computer Associates UK Ltd [2016] EWHC 1587 (QB)*, the CJEU recently held that "goods" does cover the electronic supply of computer software, and if the software is provided in return for a fee in consideration of a perpetual user licence, this will classify as a "sale of goods" for the purposes of the Directive. It now remains for the Supreme Court to decide how the CJEU judgment applies to the UK law.

As a general rule, the UK regulations will apply if the agent is performing agency services in the UK. However, the position on international agency relationships is not always simple. For example, there is scope for the parties to contract out of this if they elect the law of an EEA member state. Therefore, specific advice should be taken.

Linking, Framing, Caching, Spidering and Metatags

24. Are there any limitations on linking to a third-party website and other practices such as framing, caching and spidering?

Hyperlinking to, and framing material on, a third party's website is permitted, provided the linked material is both:

- Still publicly available.
- Not behind a pay wall of some form, or any other form of restricted access.

If the linked material has been removed or the link circumvents any subscription, pay wall or other barriers imposed by the original content owner, providing the link can be a breach of the Copyright Directive (*2001/29/EC*).

European case law also suggests that where the organisation/website linking to the material is operating for profit there may be a requirement for them to investigate whether the linked material is online with the rights owner's consent (*GS Media BV v Sanoma Media Netherlands BV, Case C-160/15*).

A recent decision of the English High Court states that where a party makes hyperlinks available to the public and that party is not a conventional search engine or website, that party may be making the works that appear at the source of the hyperlink

available to a new public without the consent of the rights holder. To assess if that is the case, regard would have to be had both to the original public and to the intended public to which the hyperlink is made available (*Warner Music and Another v TuneIn Inc [2019] EWHC 2923 (Ch)*). This decision is currently under appeal.

Other practices are not permitted if they are a breach of a third party's exclusive rights under copyright or trade mark law. Whether an infringement occurs depends on the material used and the use made of it.

In addition, if information is extracted from a third party's website, it is also necessary to ensure that the use is not in breach of the terms and conditions of that website.

25. Are there any limitations on the use of metatags or advertising keywords?

Use of metatags or keywords that are trade marks owned by a third party may infringe those trade marks. Whether or not an infringement occurs depends on the circumstances of the use. Each of the requirements necessary for trade mark infringement must be present (*section 10, Trade Marks Act 1994*) (*L'Oréal SA v eBay International AG, Case C#324/09*).

Domain Names

26. What limitations are there in relation to licensing of domain names?

There are no specific regulations in place regarding the licensing of domain names. The rules of contract law apply.

However, the licence must be in writing and signed by the licensor (the trade mark owner) if both:

- The domain name includes a trade mark owned by the registrant.
- The licensing of the domain name includes the right to use a trade mark.

(*Trade Marks Act 1994.*)

Anyone can register a ".uk" domain, whether based in the UK or not.

As a result of the UK leaving the European Union (EU), any UK-based entity that has registered a .eu domain name will no longer be entitled to hold or operate from that domain. Only EU-qualifying people or entities are entitled to register .eu domains.

27. Can use of a domain name confer rights in a word or phrase contained in it?

Domain names themselves do not confer any additional rights, but are merely property purchased by the domain name registrant from the registrar for a defined, renewable, period of time.

It is possible to register domain names as trade marks at the UK Intellectual Property Office, provided they meet the requirements for trade mark registration (and consequently the registered trade mark can also be subject to invalidation or revocation).

The use of a domain name might give rise to unregistered trade mark rights if, over time, the domain name acquires the attributes of a trade mark (for example, it serves to distinguish the goods of one undertaking from those of another undertaking). In such circumstances, if a third party misrepresents a connection or affiliation with the domain name, that third party could be committing an act of passing off. For more information, see *Practice Note: overview of passing off*.

28. What restrictions apply to the selection of a business name, and what is the procedure for obtaining one?

For the majority of company types, the trader searches the register at Companies House to ensure the proposed name of the company is not the same as, or similar to, a name that is already in use. The company name must also include the appropriate ending (for example, "Limited" or "LLP"). Company names (and changes to them) must be recorded at Companies House as part of the company registration process.

Business names that imply a connection with government or a public authority, or contain certain "sensitive" words or expressions, are restricted and must be approved by the Secretary of State. Examples of restricted words include "Queen" and "Britain".

The existence of a registered trade mark that is identical or similar to the contemplated business name should also be considered.

Jurisdiction and Governing law

29. What rules do the courts apply to determine the jurisdiction and governing law for internet transactions (or disputes)?

Jurisdiction

The same jurisdiction rules apply to internet transactions/disputes as for other disputes, although the position has recently changed following Brexit. A distinction can now be drawn between legal proceedings that:

- **Commenced before 11.00 pm on 31 December 2020.** This includes any proceedings started after this, but related to those started before. The European regime on jurisdiction (principally the Recast Brussels Regulation (*(EU) 1215/2012*), the Brussels Regulation (*(EC) 44/2001*), the **Brussels Convention of 1968**, and the Lugano Conventions of 1988 and 2007) continues to take precedence. See *Practice Note, Jurisdiction: Recast Brussels Regulation: What instruments comprise the European regime?*
- **Commenced from 1 January 2021.** The European regime no longer applies when determining a question of jurisdiction in England and Wales. The starting point is to apply the domestic law of each UK jurisdiction. For England and Wales (and subject to any future arrangements agreed between the UK and the EU), the jurisdiction of the English courts over EU-based defendants is mainly determined by:
    - the common law rules;
    - the HCCH Convention on Choice of Court Agreements 2005 (Hague Choice of Court Convention); and
    - provisions relating to jurisdiction over disputes involving consumers (or employees) contained in sections 15A to 15E of the Civil Jurisdiction and Judgments Act 1982 (CJJA).

For a detailed analysis of the differences between the jurisdictional regimes, see *Practice Note, Jurisdiction: an overview: Institution of proceedings.*

On 8 April 2020, the UK applied to accede (in its own right) to the Lugano Convention 2007. This requires the EU's agreement and it is currently unclear whether the EU will agree. It contains materially similar terms to the Brussels Regulation, except for certain amendments made under the Recast Brussels Regulation.

Governing Law

If court proceedings are commenced in a UK court, in relation to a contract, the following regulations determine governing law:

- For contracts entered into after 17 December 2009, the Rome I Regulation (*(EC) No 593/2008*), as amended by the 2019 UK Exit Regulations (*see below*), applies. See *Practice Note, Governing law: contracts made on or after 17 December 2009*.
- For contracts entered into before that date, the Rome Convention (*80/934/EEC*), as amended by the 2019 UK Exit Regulations, applies.

A core principle of Rome I and the Rome Convention is that the parties to an agreement are free to choose the law that governs that agreement. However, where the laws of a different country would have applied but for the choice of law, certain specific mandatory rules of law of that country may continue to apply.

If the parties did not choose a governing law (for example, under a sale of goods or services contract), Rome I generally provides that the law of the party selling the goods or performing the services applies, while the Rome Convention applies the law with which the contract has the closest connection. Where the contract is with a consumer, the law of the consumer's place of habitual residence generally applies (subject to exceptions which differ under the two sets of rules).

Non-contractual disputes are principally governed by the Rome II Regulation (*(EC) No 864/2007*), which is applied from 11 January 2009. As a general rule, Rome II provides that the law governing the dispute is that of the state in which the relevant damage occurred (subject to a number of exceptions).

As part of its Brexit arrangements, the UK incorporated Rome I and II into domestic law. The Rome I and Rome II Regulations, and EU-derived domestic legislation dealing with the law applicable to contractual and non-contractual obligations, are "retained EU law" within the meaning of the Withdrawal Act. Therefore, from that 1 January 2021, the UK applies the retained versions of Rome I and Rome II when determining the governing law of contractual and non-contractual obligations.

The rules under Rome I and Rome II have been amended to ensure that they operate effectively in domestic law at the end of the transition period (under the Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (UK Exit) Regulations 2019).

30. Are there any alternative dispute resolution/online dispute resolution (ADR/ODR) options available to online traders and their customers?

Legal Framework

Following Brexit, the UK's legal framework for consumer ADR and ODR is now based on domestic legislation only. This means that:

- There is no longer a requirement for UK-based ADR entities to offer cross-border services to consumers residing in EU member states.
- Traders are no longer able to offer consumers EU alternatives to UK-based ADR entities.
- The requirement for competent UK authorities to make available the list of ADR entities published by the European Commission has been replaced with a requirement to make available a list published by the UK Secretary of State.

ADR Notification Requirements

If a trader is obliged to use ADR, whether under an enactment, rules of a trade association, or terms of a contract, the trader must provide the name and website address of the relevant ADR entity:

- On its website (if the trader has one).
- In the general terms and conditions of sales or service contracts between the trader and a customer (if such terms and conditions exist).

If a trader has exhausted its internal complaint procedures following a consumer complaint (regardless of whether the trader is obliged to use ADR), they must inform the consumer on a durable medium:

- That the trader cannot settle the complaint with the consumer.
- Of the name and website address of an ADR entity competent to deal with the complaint if the consumer wishes to use ADR.
- Whether the trader is obliged or prepared to submit to an ADR procedure, operated by that ADR entity.

ODR Notification Requirements

In line with the Online Dispute Resolution Regulation (*(EU) 524/2013*), on 15 February 2016, the European Commission made an ODR platform available (*https://webgate.ec.europa.eu/odr*). This enables consumers with a complaint about a product or service bought online to submit an online complaint form to a trader who is based either within the same jurisdiction or in another country within the EU.

The Online Dispute Resolution Regulation was revoked by the Consumer Protection (Enforcement) (Amendment etc.) (EU Exit) Regulations 2018. From 1 January 2021, businesses and consumers in the UK are no longer able to use the ODR platform. UK consumers can still access ADR entities in EU countries, but not through the ODR. In addition, online traders selling in the UK are no longer obliged to provide consumers with information about the EU's ODR platform on their websites.

Remedies

The remedies available depend on the ADR provider used. It should be made clear to the users whether the ruling of an ADR provider is binding, before commencing the process.

Advertising/Marketing

31. What rules apply to advertising goods/services online or through social media and mobile apps?

The key legislation is the Consumer Protection From Unfair Trading Regulations 2008 (CPRs), which prohibit various unfair practices by traders, such as misleading actions or omissions, and aggressive sales practices. See *Practice Note, Consumer Protection from Unfair Trading Regulations 2008*.

Advertising and marketing in all non-broadcast media (including marketing claims on a company's own website, or in other non-paid-for space online under its control) is primarily governed by a self-regulatory code: the UK Code of Non-Broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code). See *Practice Note, Advertising law and regulation: content rules and enforcement: Self-regulation and co-regulation by the advertising industry*. The CAP Code includes general rules that all advertising and sales promotions must comply with, as well as certain industry-specific rules (see *Question 32*).

Outside of the field of consumer advertising, the Business Protection from Misleading Marketing Regulations 2008 govern B2B advertising, and also the conditions for lawful comparative advertising. See *Practice Note, Advertising law and regulation: content rules and enforcement: Business Protection from Misleading Marketing Regulations 2008 (SI 2008/1276)*.

Data Protection

The UK GDPR requires that all processing has a lawful basis (*Article 6, GDPR*). The Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), which remain relevant following the end of the transition period, indicate that it may be possible to rely on legitimate interests for profiling (in behavioural advertising), but that the ability to rely on this basis will diminish as the processing to build profiles becomes more invasive (for example, tracking individuals over multiple websites or platforms). Where the lawful basis of legitimate interests is not available the controller is likely to have to collect the consent of the individual being profiled. The ICO has identified behavioural advertising as a priority area for regulation and it is currently investigating ad tech and Real Time Bidding, in particular.

Any marketing conducted over direct messaging on social media is likely to be direct marketing and subject to the conditions set out in the PEC Regulations (that is, the organisation instigating the transmission of the marketing should have the consent of the individual to whom they send direct marketing unless there is an exemption). See *Question 33*.

32. Are any types of services or products specifically regulated when advertised or sold online (for example, financial services or medications)?

There are a number of types of products/services either prohibited from being advertised or sold online or subject to additional requirements under the CAP Code, such as:

- There are specific provisions regarding the online advertisement of tobacco products in the Tobacco Advertising and Promotion Act 2002, and restrictions on the sale of electronic cigarettes and refill containers in the Tobacco and Related Products Regulations 2016.
- Online gambling services require specific remote operating licences from the Gambling Commission and are subject to the restrictions in the Gambling Act 2005.
- From 1 July 2015, anybody in the UK selling medicines online to the general public must be registered with the Medicines and Healthcare products Regulatory Agency (MHRA).

33. Are there any rules or limitations relating to text messages or spam e-mails?

The PEC Regulations impose obligations on businesses that engage in direct marketing by e-mail or text message. They require senders of direct marketing e-mails or text messages to provide recipients with a valid address that can be used to opt out of further marketing communications. They also prohibit the sending of communications that disguise or conceal the identity of the sender.

Crucially, the PEC Regulations prohibit the sending of unsolicited marketing e-mails and texts to individual subscribers for direct marketing purposes, unless the recipient has consented to such communications (regardless of whether these are being sent by or merely at the instigation of the relevant business). An exception to this is the "soft opt-in", which permits a business to send marketing e-mails and texts to individual subscribers without consent where:

- Contact details have been obtained in the course of a sale or negotiations for sale.
- Direct marketing communications are in respect of that business's similar products and services.
- The recipient has been given an opportunity to opt out at the time their details were collected and is given the same opportunity at the time of each subsequent communication.

34. Does your jurisdiction impose any language requirements on websites that target your jurisdiction or whose target market includes your jurisdiction?

There are no specific language requirements for websites targeting the UK. However, section 68 of the Consumer Rights Act 2015 requires that all terms in consumer contracts or written consumer notices must be transparent. That is, they must be expressed in plain and intelligible language, and legible. This requirement is likely to prove difficult to fulfil if information relevant to the contract is not presented to a UK-based consumer in English.

Tax

35. Are sales concluded online subject to tax?

UK resident traders are subject to UK corporation tax at 19% (for companies, increasing to 25% in 2023) or income tax at up to 45% (plus National Insurance contributions) on worldwide income from sales concluded online.

A non-UK resident can be chargeable to UK taxation on profits arising from a trade carried on in (as distinct from "with") the UK, subject to double tax treaty relief. This includes non-resident companies trading through a permanent establishment (PE) (for example, a UK branch office or local employee presence). Whether a non-resident is exercising a trade in the UK is a question of fact.

In October 2021, it was agreed that the UK government would phase out Digital Services Tax (DST), which came into force in April 2020. DST applies to groups providing a social media service, internet search engine or online marketplace and is generally chargeable at 2% on the revenues of large digital businesses. Instead of DST, the UK plans to transition to the OECD's two-pillar plan to reform international corporate tax, involving a requirement on multinational businesses to transfer a portion of corporate income taxing rights from the jurisdiction of residence to the jurisdictions where economic value is in fact created.

Additional proposals include a 15% minimum level of global tax on large multinational businesses with a consolidated revenue of EUR 750 million.

The UK also has a Diverted Profits Tax (DPT) at a rate of 25% (increasing to 31% 1 April 2023). The tax is chargeable on multinational enterprises who enter into arrangements to divert profits from the UK by artificially avoiding a UK PE and/or which lack economic substance and result in a tax mismatch outcome. The DPT rules are complex but there are exceptions, including where:

- A group is a qualifying small or medium-sized enterprise.
- UK sales do not exceed GBP10 million in a 12-month accounting period.

Digital platforms remain a key focus for the UK government in seeking their co-operation to help promote tax compliance and to combat e-commerce tax fraud. In July 2021, the UK opened up a consultation on the UK's proposals for implementing the OECD's Model Reporting Rules for digital platforms. These rules will require digital platforms to send relevant information about the income of their sellers (individuals and entities) to both HMRC and the seller themselves and to undertake certain due diligence procedures. The aim is to help taxpayers get their tax compliance right and help HMRC detect and tackle non-compliance.

Online sales have UK VAT implications (see *Question 36*).

> 36. Where and when must online companies register for value added tax (VAT) (or equivalent)? Which country's VAT (or equivalent) rate applies?

Online companies with a UK establishment (for example, head office or staffed branch) generally have to register and account for UK VAT on UK sales, where turnover exceeds the UK VAT registration threshold (GBP85,000 until 1 April 2024). Overseas traders without a UK establishment must register for UK VAT if they make any taxable supplies in the UK and no VAT registration threshold applies. The UK's standard rate of VAT is 20%.

The place of supply determines where a supply of goods/services should be taxed, and in which country the registration and compliance requirements may arise. Under general rules for services, B2B services are treated as supplied where the recipient belongs. Therefore, when services are supplied by non-UK businesses to UK businesses, they usually fall within the UK's VAT reverse charge reporting procedure, requiring the business recipient to self-account for the UK VAT due. This avoids a need for the overseas supplier to register for UK VAT.

B2C services are treated as supplied where the supplier belongs under general rules, but several important exceptions apply. In particular, overseas suppliers making remote sales of B2C electronically-supplied services to UK consumers must register and account for UK VAT on those sales (no threshold). UK-based businesses are similarly liable to register and account for EU VAT on B2C electronically-supplied services to EU consumers (no threshold), although UK businesses can register under the EU's latest Non-Union One Stop Shop (OSS) system for those supplies.

For more detail, see *Practice Note, Value added tax: Place of supply*.

Significant UK VAT changes for online sales of goods were introduced as of 1 January 2021, with Great Britain no longer part of the EU Customs and VAT territory and with Northern Ireland (NI) remaining aligned with EU VAT rules for trade in goods (not services) under a complex dual VAT system under the Northern Ireland Protocol agreed with the EU as part of Brexit. As of 1 July 2021, major EU VAT changes also took effect for e-commerce sales of B2C goods and cross-border supplies of services which will affect UK suppliers selling to EU consumers and online marketplaces facilitating those sales. For details of these changes see *Practice Note, Value added tax: UK VAT law* and *Practice note: overview, Post-transition period UK VAT changes: overview*.

Under certain conditions, operators of online marketplaces in the UK may also be jointly and severally liable for the unpaid UK VAT of sellers using their platforms (similar provisions also apply in the EU), and platform operators must take certain steps in relation to the verification and publication of valid UK VAT registration numbers of those selling goods on their platforms. HM Revenue & Customs (HMRC) has powers to compulsorily register an overseas online business and/or to appoint a VAT representative and provide security.

Protecting an Online Business and Users

Liability for Content Online

37. What restrictions are there on what content can be published on a website (for example, laws regarding copyright infringement, defamatory content or harmful content)?

Content posted on a website targeted at the UK must be lawful in the UK. Some key potential areas of liability for online traders are:

- If a trader fails to comply with certain regulatory requirements (in particular regarding consumer protection), a public enforcement authority can obtain an injunction against the trader requiring it to comply with the applicable provisions (breach of which can be penalised by imprisonment or fines).
- If the trader uses third party content online without obtaining the relevant rights, it can be exposed to claims of trade mark or copyright infringement.
- Under the common law and the Defamation Acts of 1952, 1996 and 2013, where content published on a website is defamatory, the victim can obtain damages and/or an injunction requiring removal of the offending content from the website.
- There are several statutory offences that can potentially be committed through the publication of online content. For example, the publication of obscene material can be an offence under the Obscene Publications Act 1959, or the publication of racially inflammatory material an offence under the Public Order Act 1986. Criminal liability can also be incurred under the Data Protection Act where, for example, a website operator has misused an individual's personal data by publishing it online without their consent.
- Traders operating websites in the UK should also be aware of the upcoming changes relating to online harms. The UK government published a draft Online Safety Bill in May 2021, which has recently undergone pre-legislative scrutiny

and is currently being revised before the draft Bill is laid before Parliament. The current draft Bill legislates against illegal content and harmful (but not illegal) content. All platforms in scope must take measures to minimise the risk of users encountering illegal content and of children coming into contact with harmful content. Some platforms will also have to address this risk in relation to adults. In considering whether there is harmful content on their platforms, providers will have to assess whether there is a "material risk" of the content "having, or indirectly having, a serious adverse physical or psychological impact" on an adult or child "of ordinary sensibilities." The legislation will apply to any site that enables users to interact with one another and to search engines. This legislation has a relatively broad territorial scope and is not restricted to services established in the UK. Ofcom (the current UK broadcasting regulator) is to be granted wide powers to regulate Online Safety, including publishing codes of practice setting out how operators can fulfil their duties of care required under the regime, and to carry out investigations into non-compliance. Penalties under the regime include fines of up to 10% of annual global turnover or GBP18 million (whichever is higher) and the ability to order access to sites to be limited or blocked. The government has also reserved a right to introduce criminal liability for senior managers, if companies are considered not to be taking compliance with the new regime seriously.

38. Who is liable for website content that breaches these restrictions (including, for example, illegal material or user-generated material that infringes copyright or other laws, such as the law of defamation)?

Both the poster of the content and the website operator may be liable.

Whether a poster is liable depends largely on whether the website is targeted at the UK and, if so, whether the poster's activity is unlawful in the UK. If both of these factors are satisfied, the poster is liable for their content.

A website operator may also be liable (see *Question 40*).

39. What legal information must a website operator provide?

The minimum information that a website operator must provide includes:

- Name.
- Address.
- E-mail address.
- Company registration number (or equivalent means of identification).
- VAT number (if applicable).

(*Regulation 6(1)), E-Commerce Regulations.*)

UK traders must display on their website information including:

- Registered name and number.
- Address of their registered office.
- Part of the UK in which they are registered.

(*Company, Limited Liability Partnership and Business (Names and Trading Disclosures) Regulations 2015 (SI 2015/17).*)

There are additional requirements if the website is used to conclude contracts, in particular with consumers (for example, under Regulation 13 of the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013).

If the trader provides services, the Provision of Services Regulations 2009 (POS Regulations) contain further information requirements, including an obligation to provide contact details for sending complaints or requests for information (*Part 2, POS Regulations*).

A privacy notice and cookie disclosure should also be provided (see *Question 3 and Question 18*).

Additional information must also be supplied by the website operator (in certain circumstances) regarding any applicable ADR service (see *Question 30*).

The draft Online Safety Bill also appears likely to increase the amount of information that in-scope platforms must provide about how they view and treat different types of content. There has recently been a suggestion that platforms must provide an "Online Safety Policy", similar to a Privacy Policy, for users to review and agree to.

40. Who is liable for the content a website displays (including mistakes)?

A trader is liable for unlawful content displayed on its website unless it is able to rely on a defence (see, for example, Regulation 17 of the Consumer Protection From Unfair Trading Regulations (CPRs)). Unlawful content can include misleading actions or omissions of the trader, such as making misleading claims about the product, if it causes the consumer to make a transactional decision that they otherwise would not have made (*Regulations 5 and 6, CPRs*).

A similar prohibition against misleading business customers is contained in Regulation 3 of the Business Protection from Misleading Marketing Regulations 2008.

It is good practice for a trader to include disclaimers regarding the accuracy and availability of content on its website, to limit the expectations of users and therefore limit potential liability if the trader has displayed content by mistake. However, this may not be sufficient if the trader is unable to establish it has taken due care. Pricing errors are a common cause of concern. It is important that the trader's terms of sale anticipate this possibility and provide that a contract is not concluded until the trader has had the opportunity to review and confirm the order (see *Question 7*).

An information society service provider such as a website operator cannot be liable for content uploaded by a third party (that was not acting under the website operator's authority), if it:

- Does not have actual knowledge of unlawful activity or information.
- On obtaining such knowledge or awareness, acts quickly to remove or to disable access to the information.
- Immunity from liability under this Regulation applies to damages claims only; it does not protect service providers against claims involving injunctions to take down content.

(*Regulation 19, E-Commerce Regulations.*)

To benefit from this defence it is common for providers to operate a system which allows users to notify the provider of infringing content on their website, so that the provider has the opportunity to disable access to that content (a "notice and takedown" system).

Advertisers are also potentially liable for the content of their advertising that is carried out on third party websites.

The UK GDPR imposes an obligation of accuracy on the controller of any personal data (*Article 5(1)(d), UK GDPR*). The data controller is responsible for inaccuracies relating to personal data and the data subject has a right to rectification of any inaccurate data (*Article 16, UK GDPR*).

41. Can an internet service provider (ISP) shut down (or be compelled to shut down) a website, remove content, or disable linking due to the website's content, without permission?

The E-Commerce Regulations set out certain defences that ISPs can rely on to take down infringing materials such as websites, content or links (including without permission), provided that the ISPs reserve their rights in relation to these defences in the terms of their applicable agreements or terms of service.

For details of the key provisions of the E-Commerce Regulations and when they apply, see *Practice Note, Caching: Liability for caching: Electronic Commerce Regulations*.

Frequently ISPs do not disable content unless they are obliged to do so by a court order. Content owners can obtain injunctions under section 97A of the Copyright, Designs and Patents Act 1988, requiring ISPs whose services are being used by a third party to infringe copyright to block the applicable website, provided that the ISP has actual knowledge of the infringement (*Twentieth Century Fox Film Corp v British Telecommunications plc [2011] EWHC 1981 (Ch)*). The courts have also granted similar website-blocking injunctions to protect other rights such as trade marks (*Cartier International AG v British Sky Broadcasting Ltd [2014] EWHC 3354 (Ch)*) to comply with the Intellectual Property Directive (*2004/48/EC*).

The UK GDPR and DPA provide the Information Commissioner with certain powers of enforcement (*Article 58, UK GDPR*), including the power to require that a controller or a processor cease certain processing activities or cease processing certain personal data (*Article 58(2)(f), UK GDPR*).

Liability for Products/Services Supplied Online

42. Are there any specific liability rules applying to products or services supplied online?

In most cases, the position on liability for products or services supplied online is the same as for offline sales. However, online traders need to satisfy the specific requirements set out in this guide, to avoid adverse consequences. For example, where a consumer has not been informed of their right to cancel the contract, the cancellation period is extended (*Consumer Contract Regulations*).

From an intellectual property perspective, the Trade Mark Act 1994 and the Copyright, Designs and Patents Act 1988 (CDPA) also apply to acts done online. For example, the sale of a pirated work online is an infringement of section 16 of the CDPA and offering for sale goods or services that infringe a trade mark (or which the supplier has reason to believe infringe a trade mark) (see *Question 24* and *Question 41*).

See also *Question 8* about the provisions in the Consumer Contract Regulations for the supply of digital content and *Question 11* regarding remedies available for a breach of an electronic contract.

Insurance

43. What types of insurance does an online business usually need?

Online businesses largely require the same insurance as other businesses in the specific industry sector within which they operate. However, certain insurers offer products aimed at businesses with a significant online presence. For example, retailers can purchase online retailer policies which cover cyber liability as well as standard product and stock liability cover.

Reform

44. Are there any proposals to reform digital business law in your jurisdiction?

Following the UK's withdrawal from the EU, EU laws no longer have effect in the UK. Several changes have been made to retained EU law, including some provisions that have been revoked entirely. In addition, it remains to be seen whether significant upcoming reforms to the EU regime will be implemented in the UK, and the EU and UK regimes are likely to continue to diverge as their respective legislation and case law evolves separately going forwards.

Through its Digital Marketing Strategy, the EU has implemented significant legislation to promote online trade between member states. The UK Government has signalled that it does not intend to implement certain of these measures (such as the proposed Copyright Directive (*(EU) 2019/790*)) and has repealed other items of legislation that rely on the maintenance of reciprocal measures between the UK and EU member states.

Irrespective of whether it chooses to align itself with certain EU developments, the UK Government seems set to continue to review the legislative framework relating to digital business, and further reform is expected in this area in the coming years. For example:

- The draft Online Safety Bill is due to be put before Parliament for approval in 2022. This draft Bill will introduce an entirely new and strict regulatory regime governing illegal and harmful content (and possibly activity) online and will apply to user-to-user services and search engines. See *Question 37*. On 27 November 2020, the UK Government announced a new statutory framework in the UK to promote competition between digital platforms, including a code of conduct for digital platforms that will be enforced from by the newly-established Digital Markets Unit (DMU), as part of the Competition and Markets Authority, from April 2021.
- The UK Government has conducted a consultation on proposed reforms "to create an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data." The proposals include:
    - a streamlined approach to research provisions;
    - reducing the regulatory burden around AI and automated decision-making;
    - revisiting the obligations and requirements relating to DPOs and DPIAs;
    - implementing a risk-based and outcomes focused approach to international data transfers;
    - strengthening enforcement around direct marketing breaches (currently capped at GBP500,000, with a proposal to increase to UK GDPR caps);
    - allowing for DCMS to review ICO and oblige ICO to consider economic growth.

Contributor Profiles

Craig Giles, Partner

Bird & Bird LLP
T +44 020 7905 6265
E *craig.giles@twobirds.com*
W *www.twobirds.com*

Professional qualifications. Solicitor, England and Wales

Areas of practice. Commercial law; consumer law; media and sport.

Will Deller, Associate

Bird & Bird LLP
T +44 020 7415 6770
E *william.deller@twobirds.com*
W *www.twobirds.com*

Professional qualifications. Solicitor, England and Wales

Areas of practice. Commercial law; media and sport, video games, sponsorship; media rights; IP licensing, consumer law.

**The authors would like to thank Antonia Boyce (Data Protection), Caroline Brown (Tax), Rebecca O'Kelly-Gillard (IP), Graham Smith (Information Security), Gavin Punia (Payment Regulation) and Russell Williamson (Dispute Resolution) for their contribution to this chapter.*

END OF DOCUMENT

Related Content

Topics

Cookies
E-commerce
Internet

Practice note: overview

Digital marketing: an overview • Maintained

Practice notes

Domain names • Maintained
Setting up and operating a website: Contractual issues (International) • Maintained
Data Processor Obligations Under the GDPR • Maintained
Online platforms: dealings with consumers and business users • Maintained

Country Q&A

Data Protection in the UK (England and Wales): Overview • Law stated as of 30-Mar-2022
Privacy in the UK (England and Wales): Overview • Law stated as of 28-Mar-2022

