Digital business in Ireland: overview

by Adam Finlay and Sadhbh O'Sullivan, *McCann FitzGerald*

Country Q&A | Law stated as at 01-Dec-2018 | Ireland

A Q&A guide to digital business in Ireland.

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.

To compare answers across multiple jurisdictions, visit the Digital Business *Country Q&A tool*.

This Q&A is part of the global guide to digital business law. For a full list of jurisdictional Q&As visit *www.practicallaw.com/digital-business-guide*.

Regulatory overview

1. What are the relevant regulations for doing business online (for business-to-business and business-to-customer)?

Those doing business online in Ireland should be aware of a number of key pieces of domestic and EU legislation. Certain laws are specific to online business, while a significant part of the legislation in this area applies to both online and offline business contracts alike. The relevant key legislation is as follows:

- Consumer Protection Act 2007.
- Sale of Goods Act 1893 and Sale of Goods and Supply of Services Act 1980 (Sale of Goods Laws).
- European Communities (Unfair Terms in Consumer Contracts) Regulations 1995.
- European Communities (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003.
- European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013.
- European Communities (Directive 2000/31/EC) Regulations 2003 (E-Commerce Regulations).
- Electronic Commerce Act 2000.

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (Electronic Identification Regulation).
- Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)).
- Data Protection Act 2018 (Data Protection Act).
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (ePrivacy Regulations 2011).

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?

The Oireachtas (the Irish legislature) is responsible for passing legislation. It consists of the President and the two Houses of the Oireachtas:

- Dáil Éireann (the lower House).
- Seanad Éireann (the upper House).

Some primary legislative acts provide for secondary legislation to be made, typically by a Government Minister, to supplement the primary legislation.

Setting up a business online

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

Where necessary, a new online business should first consider its intended legal structure. Under the Companies Act 2014 there are several corporate vehicle options for new businesses. For example, a new business might wish to incorporate as a company limited by shares (LTD), a Designated Activity Company (DAC) or a company limited by guarantee (CLG).

The company should then look to hiring staff with relevant expertise and skills in the online sphere. This might range from the hiring of individuals to create and maintain the business website, to digital marketing specialists.

In conjunction with creating the company website, particular regard should be given to the laws regarding the collection and use of personal data under the GDPR and the Data Protection Act. For example, a website privacy notice should be implemented, along with a cookies policy, where applicable. Furthermore, the company should consider whether it is necessary in the circumstances to appoint a Data Protection Officer (DPO).

In addition, under the E-Commerce Regulations 2003, which implement Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive), certain information must be provided to website users (*see Question 37*).

The company will need to establish its terms and conditions of sale/service when dealing with its customers/users and certain information is required to be given to users of an online business (*see Question 37*).

4. What are the relevant types of parties that an online business can expect to contract with?

This largely depends on the nature of the online business. However, the following can be considered as typical agreements that an online business might enter into with third parties:

- **Development and maintenance of company website.** Examples include a Website Management Agreement or a Website Hosting Agreement.
- **IT service provider contracts.** For example, the online business might engage third parties to provide for the use of certain services or software on the company website.
- **Agreements with users/customer.** The online business may contract with those who use its website. Contracts could take the form of website terms and conditions and/or terms for the sale of goods or services.
- **General agreements relevant to the product/service being offered.** Depending on the nature of the product or service being offered, this could vary from agreements with suppliers of products, content or services, agreements with service providers and product/service distributors.

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

App development

The online business may develop the app itself or consider entering into an agreement with an app developer. This will involve determining licences for the use of relevant software and ensuring that appropriate measures are in place to deal with the ownership and use of the intellectual property (IP).

If relevant following identification of the appropriate revenue streams for the app, the online business may wish to consider concluding agreements with third-party advertisers.

App distribution
The online business may wish to engage third parties to distribute the app to users via a distribution agreement. For this purpose, the online business might consider engaging an app store to distribute the app on its behalf.

Finally, the online business may wish to enter into an agreement with its app users. Similar to the concept of a website terms of use agreement, the online business may require its app users to enter into an End User Licence Agreement (EULA).

Running a business online

Electronic contracts

> 6. Is it possible to form a contract electronically? If so, what are the requirements for electronic contract formation? Please comment on the enforceability of click-wrap, browse-wrap and shrink-wrap contracts.

Contract formation
Contracts can be formed electronically. The Electronic Commerce Act 2000 explicitly provides that, subject to limited exceptions, contracts can be concluded electronically and that an offer and acceptance can be communicated electronically unless otherwise agreed by the parties. However, any such contract is still subject to the core principles of Irish contract law (which include that for a contract to arise, generally, there must be an offer and acceptance, an intention to create legal relations and consideration).

Incorporation of the terms
There are few reported decisions of the Irish Courts in relation to the enforceability of electronic contracts. In principle, enforceable click-wrap (where usage of the product is deemed acceptance of the contract), browse-wrap and shrink-wrap contracts (containing licence agreements which are downloaded or used over the internet) are all capable of being created. However, the validity and enforceability of such electronic contracts would be subject to applicable law and, in the case of contracts with consumers, there are a number of potential obstacles to such contracts being enforceable. Shrink-wrap contracts, in particular, would be vulnerable to being held to be unenforceable against consumers on the basis that they purport to bind a consumer to contract terms with which the consumer has had no real opportunity to familiarise themselves.

The enforceability of browse-wrap contracts in a business-to-business (B2B) context was considered by the Irish Supreme Court in the 2015 decision of *Ryanair Ltd v Billigfluege.De Gmbh [2015] IESC 11*. Ryanair's browse-wrap website terms and were held to be enforceable against a third party accused of screen-scraping.

7. What laws govern contracting on the internet?

In the context of B2B, organisations must comply with obligations under the Electronic Commerce Regulations 2003. Furthermore, certain statutorily implied terms under the Sale of Goods Laws are potentially relevant. Most of these implied terms can be contracted out of in a B2B context, but not in relation to contracts with consumers.

For contracts with consumers, consumer protection legislation applicable to offline contracts also applies to contracting on the internet. In addition, the European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013 (which implement Directive 2011/83/EU on consumer rights (Consumer Rights Directive) are particularly relevant. The Regulations provide, among other things, for obligations on businesses to:

- Provide certain information to consumers.
- Provide for a 14 day "cooling off" period subject to limited exceptions.

8. Are there any limitations in relation to electronic contracts?

Electronic contracts are subject to the same general principles of Irish contract law as non-electronic contracts. However, there are certain contracts that cannot be executed electronically (*see Question 13*).

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

Personal data collected and processed via electronic contracting is subject to general data protection law principles. In this regard, the data protection laws generally applicable to electronic contracts are the same as for written, non-electronic contracts.

Under the GDPR and the Data Protection Act, personal data must only be retained by a controller/processor for as long as is necessary in relation to the purposes for which the data has been collected and/or processed. No specific guidelines as to what time periods might satisfy the requirements under the GDPR, are given. What is "necessary" can

vary depending on the particular processing activities at hand. Under Articles 13 and 14 of the GDPR, the controller/processor must inform the data subject of the period for which their personal data will be stored or the criteria for determining this.

Specific retention periods for certain records are provided for in legislation. These periods can vary greatly and the relevant primary legislation should be consulted for any specific minimum retention periods. For example, in relation to employee data, under the National Minimum Wage Act 2000, records showing compliance with the Act must be retained for a minimum of three years following the date of their making.

10. Are there any trusted site accreditations available?

There are no official government trusted site accreditations available in Ireland.

Certification Europe, an internationally-recognised accreditation body based in Dublin, certifies organisations to international standards, including the Information Security Management (ISO 27001) standard.

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

The remedies available for a breach of an electronic contract are largely the same as for offline contracts (for example, the right to termination, right to rescind, restitution, and damages).

Where certain terms implied by legislation are breached, additional remedies may be available to a consumer. For example, under the Sale of Goods Laws, and as further clarified in the EC (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003, consumers benefit from a wider range of remedies including:

- Repair/replacement.
- Reduction in price.

E-signatures

12. Does the law recognise e-signatures? To what extent and when are e-signatures used in electronic contracting? Are they required in most transactions, or very few?

Applicable legislation
The applicable laws are the Electronic Commerce Act 2000, which implements Directive 99/93/EC on electronic signatures (Electronic Signatures Directive) and the Electronic Identification Regulation (which repeals the Electronic Signature Directive). The Electronic Identification Regulation applies in parallel with the Electronic Commerce Act.

Definition of e-signatures
An electronic signature is defined in Part 1 of the Electronic Commerce Act as "data in electronic form attached to, incorporated in or logically associated with other electronic data and which serves as a method of authenticating the purported originator and includes an advanced electronic signature".

The definition given in the Electronic Identification Regulation is similar, but replaces the "method of authenticating" requirement with "data which is used by the signatory to sign".

Furthermore, under the Electronic Commerce Act, an advanced electronic signature is defined as a signature that is:

- Uniquely linked to the signatory.
- Capable of identifying the signatory.
- Created using means that are capable of being maintained by the signatory under his/her sole control.
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

While definitions of "electronic signature" and "advanced electronic signature" remain largely unchanged under the Electronic Identification Regulation, the Regulation does provide for a third type of signature: the qualified electronic signature. This means an advanced electronic signature created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Format of e-signatures
There is very little guidance on the Irish courts' interpretation of the format of electronic signatures.

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

While most contracts can be concluded using e-signatures, the execution of certain documents such as wills, trusts, enduring powers of attorney, affidavits and sworn declarations, are excluded under section 10 of the Electronic Commerce Act. Such documents must still be evidenced in the traditional form of writing. For example, while a contract for the sale of land can be concluded electronically, the deed of conveyance itself must be evidenced in the traditional form of writing.

Implications of running a business online

Cyber security/privacy protection/data protection

14. Are there any laws that regulate 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 GDPR and Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities (Data Protection Enforcement Directive), together with the Data Protection Act. Previously, the collection and processing of personal data in Ireland was governed by the Data Protection Acts 1988 and 2003.

The obligations under data protection law apply to all those who collect and process personal data (both controllers and processors of personal data). Furthermore, many rights are afforded to data subjects (the individuals whose personal data is being collected/processed).

15. What data is regulated?

Under the GDPR, personal data is defined as "information relating to an identified or identifiable natural person". An "identifiable person" is someone who can be directly or indirectly identified, by reference to an identifier such as a name, ID number, location data, an online identifier or by reference to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR further regulates the processing of more sensitive types of personal data known as "special categories of personal data". The provisions governing this type of data are more stringent and cover for example, biometric data, health data and personal data revealing a person's racial or ethnic origin or political beliefs (*Article 9, GDPR*).

16. Are there any limitations on collecting or using personal data? Are there any specific limitations on storage of personal data in the cloud?

The GDPR and the Data Protection Act place extensive obligations on those who collect and process personal data. Furthermore, several rights are afforded to data subjects.

Collection and processing of personal data

The main obligations on those collecting and processing personal data are as follows:

- Article 5 of the GDPR sets out various obligations regarding the collection and processing of personal data. Personal data must be processed lawfully, fairly and in a transparent manner. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with these specified purposes. Personal data must be adequate, relevant and limited to what is necessary in relation to these purposes and must be accurate and kept up to date. It is the data controller's responsibility to be able to demonstrate compliance with these obligations.
- A business must have a lawful basis for the processing of personal data. The legal bases for the processing of personal data are set out in Article 6 of the GDPR and include, for example, where:
    - the data subject has given their consent to the processing;
    - the processing is necessary for the performance of a contract with the data subject; or
    - the processing is necessary for the purpose of legitimate interests pursued by the controller or a third party and such interest are not overridden by the interests, rights and freedoms of data subjects.
- Article 9 of the GDPR sets out the legal bases for the processing of special categories of personal data. The special categories of personal data relate to more sensitive kinds of personal data, including, for example:
    - personal data revealing racial or ethnic origin;
    - personal data revealing political opinion;
    - genetic data; and
    - data concerning health.

    The lawful bases for the processing of such personal data include where:
    - the data subject has given explicit consent;
    - where the processing is necessary to protect the vital interests of the data subject or another where the data subject is incapable of giving consent;
    - where the processing is carried out in the course of legitimate activities; and
    - where the processing is necessary for reasons of substantial public interest.

    The GDPR specifies necessary conditions for valid consent to processing from a data subject including that consent be freely given.

Furthermore, the GDPR requires that certain information be communicated to data subjects in relation to the collecting and processing activities of a controller/processor.

Data subject rights

The collection and use of personal data is subject to data subjects exercising their rights in relation to such data. Article 13 of the GDPR requires that where personal data is collected from a data subject, certain information must be provided to the data subject. This information includes, for example:

- Details of the data controller.
- The purposes of and legal basis for the processing.
- The recipients of the personal data, if any.

Meanwhile, Article 14 sets out separate obligations regarding information that must be provided to data subjects whose personal data have not been obtained directly from the data subject.

Under the GDPR, data subjects have various rights in certain circumstances, subject to certain restrictions, in relation to personal data, including the:

- Right to access personal data.
- Right to rectification.
- Right of erasure (or right to be forgotten).
- Right to restrict the use of personal data.
- Right to object to the processing of personal data.
- Right to data portability, where the processing is based on consent or that it is necessary for the performance of a contract with the data subject.
- Right not to be subject to automated decision making.

A controller is obliged to respond to requests exercising the rights above without undue delay and in any event within one month of receipt of the request from the data subject, subject to limited exceptions provided for under the GDPR and the Data Protection Act.

Personal data held in the cloud

There are no additional obligations imposed specifically in relation to the storage of personal data on the cloud. However, any agreement concluded with cloud service providers will need to comply with the principles of data protection law. These would include the requirement that there be a contract in place which contains certain mandatory provisions that must be imposed by a controller regarding the processing of personal data by a third-party processor on its behalf.

17. Is the use of cookies allowed? If so, what conditions apply to their use that impact system design?

The use of cookies is allowed subject to compliance with the applicable conditions. The law related to the use of cookies is set out in the ePrivacy Regulations 2011, which implement Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive).

Under Regulation 5(3) of the ePrivacy Regulations, an electronic communications network cannot be used to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless both:

- Consent has been given by the subscriber/user.
- The subscriber/user has been provided with relevant information in accordance with data protection law.

Regulation 5(4) requires that the methods for providing information and giving consent should be as user-friendly as possible. Users' consent to the storing of information or gaining access to information already stored can be given by the use of browser settings or other technological means by which the user can be considered as having given consent. However, reliance should not be placed on default browser settings.

Following review of the E-Privacy Directive, the European Commission published its proposal for a new E-Privacy Regulation in January 2017, which will replace the current E-Privacy law regime throughout the EU. The text of the Regulation, which is intended to complement the GDPR, is currently still under review and includes updated rules related to cookies.

18. What measures must be taken by contracting companies or the internet providers to guarantee the security of internet transactions?

The ePrivacy Regulations 2011 impose obligations on providers of publicly available e-communication networks or services to take appropriate technical and organisational measures to safeguard the security of its services. However, it should be noted that the new proposed ePrivacy Regulation is still under review and is intended to overhaul the law in this area (*see Question 17*).

In relation to the protection of personal data which might be implicated by internet transactions, Article 32 of the GDPR is relevant. This requires a controller and a processor of personal data to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved. Several factors must be considered when determining the appropriateness of measures, including the costs of implementation and the nature, scope, context and purposes of processing.

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (Network and Information Security Directive) requires member states to ensure that digital service providers identify and take appropriate and proportional technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services (such as cloud computing services for example). Such measures must ensure a level of security appropriate to the risk posed and take into account a number of elements. The Network and Information Security Directive was

transposed into national law by the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.

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

While the GDPR does not explicitly require encryption in any particular circumstance, the technical and organisational measures to be taken under Article 32 (*see Question 18*) include the pseudonymisation and encryption of personal data, where appropriate. Pseudonymisation of data is the process of replacing any identifying characteristics of data with a pseudonym, or in other words, a value that does not allow the data subject to be directly identified. Encryption renders the data unintelligible to those who are not authorised to access it.

Several factors must be considered when determining the appropriateness of measures, including the costs of implementation and the nature, scope, context and purposes of the processing.

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

The Data Protection Commission (DPC) can serve an information notice on a controller or processor, requiring him/her to furnish the DPC with such information as is necessary or expedient for the performance by the DPC of its functions in relation to its investigation and enforcement under Part 6 of the Data Protection Act (such as details of how the controller or processor ensures compliance with its obligations under data protection law). This obligation does not, however, extend to information covered by legal professional privilege (such information is not admissible in evidence in court proceedings for an offence outside of this section).

The Communications (Retention of Data) Act 2011 requires service providers to retain telephony and internet data for specified periods. The Act further compels service providers to comply with requests for disclosure of data to (where necessary):

- The Garda Síochána.
- The Permanent Defence Force.
- The Revenue Commissioners.
- The Competition and Consumer Protection Commission (CCPC).

However, the Communications (Retention of Data) Act implements Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive), the Act has been declared invalid by the Court of

Justice of the European Union (CJEU) in the *Digital Rights Ireland* ruling (joined cases *C-293/12* and *C-594/12*). While the Communications (Retention of Data) Act currently remains in force in Ireland, the Government recently published the general scheme for the new Communications (Retention of Data) Bill 2017.

More generally, various government bodies and public authorities can compel the disclosure of personal data and other information in the performance of their public powers or functions.

21. Are there any regulations in relation to electronic payments?

The European Union (Payment Services) Regulations 2018 implement Directive (EU) 2015/2366 on payment services in the internal market (PSD2) in the internal market. These new rules govern electronic payments and include strict security requirements for electronic payments and for the protection of consumers' financial data.

22. If the site is aimed at children, are there any specific rules or guidance that apply?

There is a general transparency obligation under the GDPR which requires that where the processing is addressed to a child, it should be in such a clear and plain language that the child can easily understand.

Under section 31 of the Data Protection Act, the digital age of consent in Ireland for the purposes of Article 8 GDPR is 16 years old. This means that where the processing of personal data relating to a child under the age of 16 years in connection with the provision of information society services to the child is to be based on consent, the consent must be given or authorised by a person with parental responsibility over the child.

Under Article 6(1)(f) of the GDPR, where an organisation intends to rely on "legitimate interests" as its legal basis for processing, it must consider whether such interests should be overridden by the interests or fundamental rights and freedoms of the data subject "in particular where the data subject is a child".

The Data Protection Act also contains a proposed provision under which it would be a criminal offence for any company or corporate body to process the personal data of a child under the age of 18 years for the purposes of direct marking, profiling or micro-targeting. However, this provision has not been brought into force and its validity is under consideration by the Irish Government.

If a website purports to enter into a contract with a minor (that is, a person under the age of 18 years), the general common law principles applicable to the conclusion of contracts with minors are relevant. In general, a contract with a minor will not be enforceable against the minor unless it is a contract for "necessaries" or a contract for education, apprenticeship or service.

Linking

23. Are there any limitations on linking to a third party website and other practices such as framing, caching, spidering and the use of metatags?

While there is no general legislative prohibition on linking to a third-party website at domestic or EU level, any such linking is subject to certain limitations and must not infringe the IP rights of any third party.

Issues can often arise in the context of copyright infringement, requiring a determination of whether the particular act amounts to a "communication to the public" under the meaning of Article 3 of Directive 2001/29/EC on copyright and related rights in the information society (Copyright Directive). Linking to third-party websites is generally acceptable, provided the:

- Content is publicly available and there is no "new public" gaining access to the content.
- Content was published with the content owner's consent on another website.
- Person posting the link does not seek financial gain.
- Personal posting the link acts without the knowledge that the content has been published illegally.

In the context of framing, the CJEU's decision in *Bestwater International GmbH v Mebes* (*Case C-348/13*) is instructive. Here, the CJEU found that framing did not amount to a "communication to the public" where there was no transmission to a "new public".

Domain names

24. What regulations are there in relation to licensing of domain names?

There are no specific regulations dealing with the licensing of domain names. However, when choosing a domain name for a business website, it is necessary to first check the relevant domain registry (IE Domain Registry) to see if the domain is available for use. Furthermore, even if the domain name is available on the registry, it is still necessary to check whether the relevant name might be affected by any trade mark protection.

The IE Domain Registry requires applicants for .ie domain names to demonstrate some connection to the island of Ireland.

25. Do domain names confer any additional rights (in relation to trade marks or passing off) beyond the rights that are vested in domain names?

Domain names do not confer any additional rights in themselves. It is possible to secure trade mark protection for a domain name and this protection would confer additional rights to the trade mark owner.

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

When registering a new company with the Companies Registration Office (CRO), certain restrictions apply to the selection of a company name. The CRO may refuse a name if:

- The name is identical or too similar to an existing business name on the register of companies.
- The name is offensive.
- The name suggests state sponsorship.

Furthermore, names containing certain words such as "bank", "society" or "University" cannot be used unless approved by the relevant bodies. It should also be noted that, while the registration of business names ending in a domain name suffix is considered undesirable, it is possible to register such names.

Before applying to register a business name with the CRO, applicants should check that the proposed name is not similar or identical to a name already registered. The CRO does not check proposed names against those registered on the business names register or trade mark register. These should be checked separately to ensure that, for example, there is no risk of a passing off action being taken against the business.

Registration of a business name is obligatory if any individual or partnership or body corporate carries on business under a name other than their true name. Registration is completed by filling out a form RBN1 (individual), RBN1A (partnership) or RBN1B (body corporate) and submitting the form along with the relevant registration fee to the CRO.

Jurisdiction and governing law

27. What rules do the courts apply to determine the jurisdiction for internet transactions (or disputes)?

The relevant legislation dealing with the determination of jurisdiction in cross-border contracts at EU level is Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast Brussels Regulation). This replaces the earlier Regulation (EC) 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Regulation) and addresses jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

Article 4 of the Recast Brussels Regulation provides that a person domiciled in a member state, regardless of their nationality, will be sued in the courts of that member state. Article 7 of the Recast Brussels Regulation provides for situations where a person can be sued in a member state they are not domiciled in. This includes, for example, in matters related to contract, in the courts of the place where the contract is performed.

Article 25 of the Recast Brussels Regulation provides that an agreement of the parties as to jurisdiction takes precedence, unless that agreement is null and void under the law of that member state.

Article 25 further provides that an agreement conferring jurisdiction must take a certain form to be considered enforceable. One such prescribed form is "in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known". The Irish High Court recently considered whether a jurisdiction clause contained in a website's terms of use could bind parties to the named jurisdiction, and in finding that there had been such agreement as to jurisdiction, held that "there is a practice in the airline and online travel agency sectors of contractually binding web users by click wrapping or browse wrapping, which practice is generally and regularly followed by the operators in those sectors" (*Ryanair Limited v On the Beach Limited* [*2013] IEHC 124*). Furthermore, in 2015 the CJEU confirmed the validity of accepting jurisdiction clauses for the purposes of Article 25 of the Recast Brussels Regulation, through click-wrapping (*Jaouad El Majdoub v CarsOnTheWeb.Deutschland GmBH Case C-322/14*).

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

In relation to the choice of governing law for internet transactions, the relevant legislation is Regulation (EC) 593/2008 on the law applicable to contractual obligations (Rome I). This provides for certain default rules where no choice as to governing law has been made:

Article 3 of Rome I provides that a contract will be governed by the law chosen by the parties to the contract. The parties can select the law applicable to the whole or part of the contract. However, under Article 3(3), if all other elements relevant to the contract other than the choice of governing law are located in a country other than the country selected by the parties, the provisions of law of the other country which cannot be derogated from by agreement, will still apply regardless of the parties' choice.

Article 4 provides default rules for when no choice as to governing law has been made by the parties. For example, a contract for the sale of goods/services will be governed by the law of the country where the seller/service provider habitually resides.

29. Are there any alternative dispute resolution / online dispute resolution (ADR/ODR) options available to online traders and their customers? What remedies are available from the ADR/ODR methods? Are there any requirements to notify customers of the availability of these methods?

The options available to online traders and customers in relation to ADR and ODR largely stem from laws established at EU level.

The relevant legislation dealing with ADR options is the European Union (Alternative Dispute Resolution for Consumer Disputes) Regulations 2015 (SI 343/2015). These Regulations implement Directive 2013/11/EU on alternative dispute resolution for consumer disputes (ADR Directive) and apply to domestic and cross-border contractual disputes arising from sales contracts or service contracts between traders established in the EU and a consumer resident in the EU.

Under Regulation 18, a trader who has committed or is obliged to use an ADR entity in the resolution of disputes with consumers, must inform consumers of the relevant ADR entity covering the trader's sector and provide details of the website address of the entity. This information must be provided to the consumer on the trader's website and in the general terms and conditions of sale or services contracts with the consumer. Such information must be provided to a consumer in writing where the consumer has submitted a complaint directly to the trader that could not be settled. Failure to comply with Regulation 18 can lead to a class A fine and/or 12 months imprisonment.

The remedies available depend on the ADR entity that is engaged. The CCPC maintains a public list of ADR entities.

The relevant legislation dealing with ODR options is the European Union (Online Dispute Resolution for Consumer Disputes) Regulations 2015. These Regulations implement Regulation (EU) 524/2013 on online dispute resolution for consumer disputes (Online Dispute Resolution Regulation). The European Commission has established an ODR platform through which consumers and traders can settle contractual disputes in relation to domestic and cross border purchases made online. The designated ODR contact point for Ireland is the European Consumer Centre Ireland.

In relation to the requirements for notifying consumers, traders engaging in online sales or service contracts and online marketplaces within the EU must provide a link to the ODR platform on their website, along with their email address information. Meanwhile, a trader who has committed or is obliged to use an ADR entity must inform

consumers of the existence of the ODR platform and provide a link to this on their website, or by email if the offer is made by email. This information should also be provided for in their general terms and conditions.

Advertising/marketing

30. What are the relevant rules on advertising goods/services online/via social media?

The rules for advertising online can be found in the Code of Standards for Advertising and Marketing Communications in Ireland (Code), issued by the Advertising Standards Authority for Ireland (ASAI). The Code is a non-binding code of practice. Particularly relevant are:

- Section 6, which deals with distance selling.
- Section 18, which deals with online behavioural advertising.

In 2016, the ASAI published guidance in relation to marketing communications (Marcoms) on social media. The guidance confirms that the Code applies to all types of Marcoms, including communications made via social media. The guidance provides for a general rule whereby all Marcoms must be clearly identifiable as being such. The rule requires bloggers and influencers for example, to flag Marcoms in their social media posts so that consumers are aware that content is a Marcom prior to engaging with online content. The relevant test for a Marcom is whether the content has been paid for and controlled by the advertising company.

31. Are there any types of services or products that are specifically regulated when advertised/sold online (for example, financial services or medications)?

Certain products are specifically regulated and for which the rules will apply in both an online and offline context. These include food and non-alcoholic beverages, alcoholic drinks, gambling, health and beauty products, financial services/products and e-cigarettes.

32. Are there any rules or limitations in relation to text messages/spam emails?

The ePrivacy Regulations 2011 are relevant in the context of sending unsolicited text or email communications. For example, under Regulation 13, a person must not send an unsolicited email communication to another for the purposes of direct marketing unless the sender has been notified by the individual that they consent to such communications. This rule does not apply in relation to corporate email address where the purpose of the direct marketing relates solely to the person's work context. There is also a limited exception for a business sending marketing emails to its existing customers regarding its own products or services based on the absence of an opt-out in certain circumstances, which is known as the "soft opt-in". However, the current ePrivacy rules are due to undergo significant reform in light of proposed "E-Privacy Regulation" which is currently under review at an EU level. Once finalised, this Regulation will have direct effect and replace the current ePrivacy law regime.

Separately, in the context of the GDPR, any business that processes personal data for direct marketing must have a legal basis for doing and must have notified the relevant individuals of this intended processing of their personal data and their rights as data subjects in relation to such processing (including the right to object).

33. Are there any language requirements in your jurisdiction for a website that targets your particular jurisdiction or whose target market includes your jurisdiction?

Generally, there are no such requirements, except for websites published by Irish public authorities (which must also be published in the Irish language).

Tax

34. Are sales concluded online subject to taxation?

Worldwide income from sales concluded online is within the scope of Irish taxation for Irish resident traders subject to Irish corporation tax at 12.5% for companies, or income tax at a rate of up to 40% (plus Universal Social Charge (up to 8%) and Pay Related Social Insurance contributions (up to 4%)).

A non-Irish resident can be chargeable to Irish taxation on profits arising from a trade carried on in Ireland, subject to double taxation treaty relief. This includes non-resident companies trading through a permanent establishment (PE) (for example, an Irish branch office or local employee presence). Whether a non-resident is exercising a trade in Ireland is a question of fact. One key factor (both in determining the place of trade and whether there is a PE) is the

place where the online contract is made. However, the Organisation for Economic Co-operation and Development base erosion and profit shifting project has proposed widening this to also include the place where the principal role leading to the conclusion of the online contract is carried out (where material negotiations take place). Further, even in cases where contracts are made abroad, a trade is exercised in Ireland if there is otherwise substantial profit-making activity performed in Ireland.

Online sales will also have VAT implications (*see Question 35*).

35. Where and when must online companies register for VAT and other taxes? Which country's VAT rate will apply?

Online companies with an Irish establishment (for example, head office or staffed branch) must register and account for Irish VAT on Irish sales where turnover exceeds the VAT registration thresholds, presently:

- EUR37,500 for persons supplying services.
- EUR75,000 for persons supplying goods.

Different thresholds apply in some other specific circumstances, such as a person making acquisitions from other EU member states (EUR41,000).

Overseas online traders must register for Irish VAT if they make any taxable supplies in Ireland even without an Irish establishment, depending on the nature of the product they sell.

Cross-border trade in services within the EU between businesses broadly fall within a VAT reverse charge reporting procedure, which requires the business customer to self-account for the VAT due which avoids a need for the supplier to VAT register in the business customer's country. A similar regime exists in relation to goods.

Different rules apply for cross-border business-to-customer supplies (B2C) within the EU, for example:

- All suppliers of B2C digital services must register and account for VAT on their B2C sales in each EU country where their customers are located, at the VAT rate applicable in their customer's country. Businesses face compliance burdens in establishing their customer location. To help reduce a supplier's administrative burden, an optional Mini One Stop Shop (MOSS) system has been introduced. This allows a supplier to register electronically in one EU country and submit single quarterly VAT returns and payments due in other EU countries, in which the supplier does not have an establishment.
- EU businesses are subject to distance selling rules for cross border B2C sales of goods, requiring suppliers to register for VAT in their EU customer's country where the value of B2C sales exceeds that country's distance selling threshold (EUR35,000 for distance sales into Ireland).

Goods brought into Ireland from outside the EU are not distance sales or acquisitions but imports potentially chargeable to import VAT. Goods removed from Ireland are potentially VAT-free exports if removed to a non-EU jurisdiction within applicable time limits and supported by necessary evidence of removal.

Companies establishing in Ireland must first obtain a CRO number to register for VAT and other taxes. Once a CRO number is obtained, the company can use the Revenue Online Service (ROS) to register for Corporation Tax, Employer Pay-As-You-Earn (PAYE) and VAT, as applicable.

Protecting an online business

Liability for content online

36. What laws govern liability for website content?

If an online trader does not own all the rights to its website content (for example the copyright to images, music or software used, or trade mark protected material), the permission to exploit such materials must first be obtained. This may take, for example, the form of a licence concluded with the content owner. Failure to take such steps risks leaving the online trader susceptible to legal actions for IP infringement. Furthermore, online traders should be careful about linking to third-party content (*see Question 23*).

An online trader must not post any content that could be deemed defamatory within the meaning of the Defamation Act 2009.

Furthermore, there are certain statutory offences which might be relevant in relation to the publication of online content. For example, an online trader must not post content which interferes with any individual's personal data or privacy rights under data protection law and other applicable law. A further example includes the publication of material likely to stir up hatred under the Prohibition of Incitement To Hatred Act 1989.

37. What legal information must a website operator provide?

Regulation 7 of the Electronic Commerce Regulations 2003 requires a website operator to provide certain information, including its:

- Name.
- Address.
- Contact details (email address).

- Company registration number (or other registration number where relevant).
- VAT number.

Furthermore, under Irish company law, limited liability companies who operate a website must display certain information to users, including:

- The name and legal form of the company.
- The place of registration of the company and its registration number.
- The address of the company's registered office.
- In the case of a company exempt from the obligation to use the company type (Companies Limited by Guarantee/Designated Activity Companies) as part of its name, the fact it is such a company.
- In the case of a company which is being wound up, the fact that it is being wound up.
- If the share capital of a company is mentioned on the website, the reference must be to the issued share capital.

Under data protection law, a website operator must make available a website privacy notice in relation to the personal data it collects from individuals using its website.

While not mandatory, a website operator might wish to include terms and conditions of use of its website.

If a website operator seeks to conclude distance contracts with its website users, it must provide certain information under Regulation 11 of the European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013.

Furthermore, where applicable, certain information must be published to the website in the context of ADR/ODR options (*see Question 29*).

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

Generally, an online trader who posts content on their website is liable for such content.

Internet Service Providers (ISPs) providing a platform for User Generated Content (UGC) may be in a position to use the hosting exemption under Regulation 18 of the Electronic Commerce Regulations 2003. This exemption applies only where both:

- The ISP does not have actual knowledge of the unlawful activity (that is, the copyright infringing content).
- On learning of the unlawful activity, the ISP acts expeditiously to remove or disable access to this content.

Satisfying this test, the ISP will not be found liable, as it is considered as having a passive role in the committal of the relevant unlawful activity.

An online trader who posts product information on its website should be aware of the prohibition on unfair and misleading commercial practices under the Consumer Protection Act 2007.

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

An ISP can, without permission, shut down a website, remove content, or disable linking if its applicable terms and conditions permit this. Alternatively, an ISP may be required by law to take such action. Under section 40(5A) of the Copyright and Related Rights Act 2000, on the application of a copyright owner, the High Court may grant an injunction against an intermediary in the context of infringement of copyrighted material. In the past, this section has been invoked to issue website blocking orders as against non-infringing intermediaries, for example in the case of *EMI Ireland Records Limited v UPC Communications Ireland Limited [2013] IEHC 274*.

Liability for products/services supplied online

40.Are there any rules that might apply to products or services supplied online?

The rules for products and services supplied online are generally the same as for the offline supply of goods and services. However, some legislation applies specifically to online contracts concluded for the sale of goods and supply of services (*see Question 7*). For example, under the European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013, subject to limited exceptions, consumers are entitled to a 14-day cooling off period during which they may cancel a distance contract or off-premises contract (which includes online contracts).

Insurance

41. How should an online business be insured?

Generally, an online business will require the same types of insurance as an offline business. Depending on the nature of its business activities, an online business may wish to secure additional, more specialist insurance, such as cyber insurance, which would cover other core risks (for example, data liability).

Reform

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

At present, there are several key pieces of draft legislation circulating at various stages of the legislative process:

- Copyright and other Intellectual Property Law Provisions Bill 2018 (*see www.oireachtas.ie/en/bills/bill/2018/31/*).
- Digital Safety Commissioner Bill 2017.
- A Cyber Security Bill and Cyber Crime Bill are both listed in the Government's Spring/Summer 2018 Legislative Programme. (*see www.taoiseach.gov.ie/DOT/eng/News/Government_Press_Releases/Government_Legislation_Program_Spring_Summer_2018.html*).
- The ePrivacy Regulations 2011 are due to be reformed in light of the proposed ePrivacy Regulation which is currently being reviewed at an EU level (*see also Question 32*).
- The General Scheme of the Communications (Retention of Data) Bill 2017.
- Data Sharing and Governance Bill 2018.

Online resources

Advertising Standards Authority for Ireland (ASAI)
W *www.asai.ie*

Description. The official website of the ASAI.

Companies Registration Office Ireland (CRO)
W *www.cro.ie*

Description. The official website of the CRO.

Data Protection Commission
W *www.dataprotection.ie*

Description. The official website for the Data Protection Commission, Ireland's national supervisory authority for the purposes of the GDPR.

Irish Statute Book (ISB)
W *www.irishstatutebook.ie*

Description. An online searchable database of all primary and secondary legislation in Ireland.

Contributor profiles

Adam Finlay, Partner

McCann FitzGerald

T +353 1 607 1795
E *adam.finlay@mccannfitzgerald.com*
W *www.mccannfitzgerald.com/people/adam-finlay*

Sadhbh O'Sullivan, Associate

McCann FitzGerald

T +353 1 607 1234
E *sadhbh.osullivan@mccannfitzgerald.com*
W *www.mccannfitzgerald.com*

END OF DOCUMENT

