International
Comparative
Legal Guides

Digital Business 2020

A practical cross-border insight into digital business law

First Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Armengaud Guerlain
Bagus Enrico & Partners
BOEHMERT & BOEHMERT
Boga & Associates
Bull & Co
Cliffe Dekker Hofmeyr
Cozen O'Connor P.C.
E & G Economides LLC
Gowling WLG
Greychapel Legal
Hammad & Al-Mehdar Law Firm
Hassan Radhi & Associates
Lewis Silkin
Orchards
Portolano Cavallo
Shin Associates
Sirius Legal
Veirano Advogados
Walder Wyss Ltd

ICLG.com

ISBN 978-1-83918-051-4
ISSN 2732-5237

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Group Publisher
Rory Smith

Publisher
James Strode

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Business 2020

First Edition

Contributing Editors:
Davey Brennan & Alex Brodie
Gowling WLG

©2020 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Chapter

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the first edition of the *ICLG – Digital Business*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to laws and regulations relating to digital businesses around the world, and is also available at www.iclg.com.

The question and answer chapters, which in this edition cover 21 jurisdictions, provide detailed answers to common questions raised by professionals dealing with digital business laws and regulations.

The publication's opening expert analysis chapter provides further insight into navigating business digitalisation.

As always, this publication has been written by leading lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editors Davey Brennan and Alex Brodie of Gowling WLG for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Ireland

Lewis Silkin

Victor Timon

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

B2B e-commerce in Ireland is treated very much the same as non-ecommerce B2B business, in that much of the same legislation will apply. So, the Sale of Goods Act 1893 and Sale of Goods and Supply of Services Act 1980 would be the basic legislation covering either type of transaction. These include a buyer's rights in terms of merchantable quality, right to free possession and the like.

However, there are some laws that apply particularly to e-commerce transactions. These are a mix of directly applicable EU law and Irish implementations of EU legislation.

The Electronic Commerce Act 2000 regulates the manner in which business is to be conducted online and introduced electronic signatures.

The European Communities (Directive 2000/31/EC) Regulations 2003 (E-Commerce Regulations) further governs the use of online contracts.

The Eidas Regulation ((EU) 910/2014) regulates electronic signatures and electronic transactions, to provide a safe way for conducting business online.

The General Data Protection Regulation (Regulation (EU) 679/2016) also applies as does the Data Protection Act 2018 (DPA), which transposes its provisions into Irish law.

Ireland is also subject to the Geo Blocking Regulation (Regulation (EU) 2018/302) for online (and offline) sales under which a trader may not restrict access to its website through the use of geo-factors such as location or IP address.

The new Copyright Directive 2019/790 must be transposed into Irish law by 7 June 2021 and is intended to make copyright fit for the digital age. It gives content creators new rights to be rewarded for their efforts through licensing arrangements with information society service providers (ISSPs). It imposes new responsibilities on ISSPs and other platform providers to negotiate those licences fairly. It also obliges them to prevent infringing content appearing in their services or on their platforms.

There is no registration required in Ireland in general to conduct an e-commerce business, though see question 11.2 for the regulations applicable to online payment providers.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

The legislation described in question 1.1 will also apply to B2C e-commerce transactions, but there are also additional legal provisions which are designed to protect consumers.

The Consumer Protection Act 2007 provides general protection for consumers in transacting with traders either through e-commerce or offline. These include provisions which prohibit a trader making false claims about a product or service. It also prohibits misleading advertising. In all, the Act lists 32 practices which are prohibited, backed up by a series of fines and other enforcement measures.

The European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013 implemented Directive 2011/83/EU (the Consumer Rights Directive) in Ireland. It governs so-called "distance contracts". The Regulations provide consumers with a 14-day "cooling off period" during which they can change their mind and cancel a purchase (with limited exceptions, such as for perishables and digital products). Goods must be delivered in 30 days. A trader cannot force a consumer to use a premium rate phone number in connection with his/her purchase.

In addition, the Regulations set out the information which a trader must provide to a consumer, such as a full description of the goods, the total price including any taxes and certain information required to identify the trader.

The European Communities (Unfair Terms in Consumer Contracts) Regulations 1995 (as amended) introduced a test of fairness for consumer contracts. They require that standard terms are written in plain and understandable language. The Regulations list certain terms that could be considered unfair, for example terms which provide for an automatic renewal of a contract without the consumer's agreement.

The European Communities (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003 further strengthened a consumer's rights. They stipulate that goods must comply with their description and provide for repair and replace remedies where that is not the case.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

It is now two years since the GDPR came into force in Ireland, and while there have been no major domestic developments in that time, the Data Protection Commission's (DPC) Annual Report issued in February 2020 showed some interesting trends since its introduction.

In the calendar year 2019, complaints to the DPC increased by 75%, reflecting perhaps an increased awareness of a data subject's rights. Telecommunications companies and banks remain the most complained about organisations.

Valid data breaches notified to the DPC in 2019 were up 71% from 2018. Unauthorised disclosures made up 83% of breaches, with an increase in the number of repeat breaches of a similar nature by a large number of organisations (predominantly in the financial sector).

In 2019, the DPC had 70 ongoing statutory inquiries, including 21 cross-border inquires. In the technology sector, the DPC is currently involved in six statutory inquiries in relation to several high-profile multinational tech companies.

Decisions and fines from two enquiries into "big tech" companies are expected later in 2020.

Having considerably increased its manpower and resources in the last year, the DPC has become much more active in relation to investigations and prosecutions. An example of this can already be seen in the area of direct marketing offences. Offences in this area were pursued rigorously in 2019 and 165 new complaints were investigated. Expect to see even more activity in this area in the coming years.

The DPC is the lead supervisory authority for a number of multinationals, and under the "One Stop Shop" (OSS) system set out in the GDPR. As a result, the DPC received 457 cross-border processing complaints under the OSS which were lodged by individuals via other EU data protection authorities last year.

The DPC spent significant time engaging with stakeholders to provide information on Brexit, particularly in relation to Irish companies transferring personal data to the UK.

In April 2020, the DPC issued a report and guidance on the use of cookies. It found widespread non-conformance based on a survey of 38 organisations.

The DPC found that controllers had a poor understanding of the 'necessary' or 'strictly necessary' exemption. The DPC stressed that the exemption is extremely narrow and can only apply to a service that has been explicitly requested.

The DPC states in its guidance that consent for cookies should be limited to a timespan of six months, after which time consent should be refreshed. It also stressed the need for transparency.

It has allowed a six-month time period for controllers to comply with the new guidance, after which they say action will be taken.

In May 2020, the DPC issued its first fine under GDPR. Tulsa, the State's child and family agency, was fined €75,000 for three data breaches.

The DPC is also carrying out separate enquiries into the ad-tech sector, and it is expected that guidance on this will be issued later in 2020.

2.2 What privacy challenges are organisations facing when it comes to fintech, AI and digital health?

FinTech

Privacy challenges faced by fintech companies are not dissimilar to those in other industries. However, one key area where they may be ahead of other industries is the drive to use biometric data to increase security. Biometric data is regarded as "special category data" under Article 9 of the GDPR (section 2/45 DPA). As such, it would require the explicit consent of the data subject before it could be processed.

The systems for deploying biometric data would need to be developed on the basis of "privacy by design" set out in Article 25 of the GDPR (section 76 DPA), which requires embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage.

It is also likely that a Data Protection Impact Assessment would need to be carried out and documented under Article 35 of the GDPR (section 84 DPA) to analyse the risks involved for a data subject's rights and to determine if a deployment could go ahead based on the benefits involved.

Many fintech companies operating in Ireland are part of much bigger international organisations and they face the challenge of ensuring that any transfers of data outside of the jurisdiction meet the requirements for international transfers under Chapter 5 of the GDPR (Chapter 5 DPA).

Brexit may be a challenge if at the end of transition, the UK leaves on a no-deal basis. In such a scenario, and in the then likely absence of an adequacy decision, fintech companies with affiliates, customers or service providers in the UK would have to review the transfer of personal data from Ireland to the UK. The UK would be regarded as a third country in that event, and safeguards such as the Standard Contractual Clauses or Binding Corporate Rules would need to be put in place as required by Articles 46 and 47 of the GDPR (section 98 DPA).

Finally, those fintech companies based outside of Ireland but marketing their services to Irish citizens will also have to comply with the GDPR.

AI

Due to the very nature of AI, there seems to be two aspects of the GDPR which are going to be regularly applicable.

The first is Article 25 of the GDPR (section 76 DPA) which obliges a controller to build privacy by design and default into any new systems.

The second is Article 35 (section 84 DPA) which states that where a type of processing uses new technologies, likely to result in a high risk to the rights and freedoms of people, the controller must carry out a risk assessment. In particular, for instances of automated processing on which decisions are based that produce legal effects, a DPIA must be conducted.

In deploying an AI system, a company will also have obligations pursuant to Article 22 (sections 57/89 DPA) and the European Data Protection Advisory Board's guidance to explain the logic behind an automated processing system. In terms of transparency, a controller will need to explain its processing anyway. Where the machine itself is making the rules, that may be difficult.

The fact that a machine may make decisions without human involvement may make any need to obtain specific consent much more difficult, unless of course that too is built into the algorithm.

While in the UK the ICO has issued guidance on how to explain AI decisions to data subjects, so far there has been no similar advice in Ireland.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Digital Health
Health data classifies of course as special category data under Article 9 of the GDPR (section 2/45 DPA), and so needs special protection.

As Ireland's health system continues to adopt more technological solutions and moves further away from an unconnected and manual approach, it will face the same challenges as other industries in terms of cyber security and protection of information that is now stored in the cloud.

New digital technologies that allow for remote patient monitoring, consultations by video link, and real-time data being obtained from medical devices and wearables, with the ensuing increase in the volume of data, will undoubtedly provide more privacy and security challenges.

Stakeholders in the digital health industry, whether controllers or processors, will need to continually review their internal procedures, training and technology to ensure that they can meet the demands of an explosion of data and data sources.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, AI and digital health?

There are government and government agency initiatives for the development of products in these areas. None of these is particularly steered towards testing.

In fintech, the Government's IFS2020 programme was established in 2015 to support the development of fintech products. The Central Bank of Ireland (CBI) also runs an innovation hub.

In respect of the development of AI products, CeADAR is an AI innovation hub supported by two government agencies, Enterprise Ireland and IDA Ireland.

For digital health products, the Health Innovation Hub Ireland was established by the Department of Business, Enterprise and Innovation and the Department of Health, supported by Enterprise Ireland (EI) and the Health Service Executive (HSE) to drive collaboration between the health service and enterprise.

The DPC does not play any defined statutory role in the development or testing of such products, other than its overriding role of enforcing the GDPR. In particular, the DPC has issued guidance in respect of the situations in which it believes a DPIA should be carried out.

In addition, where a DPIA is required for the deployment of any of this type of products and, following its completion any identified risks cannot be managed and the residual risk remains high, then the instigator of that DPIA is obliged, pursuant to Article 36 of the GDPR (section 84 DPA), to consult with the DPC for its opinion before progressing with the project.

Even if a consultation is not required, the DPIA can of course be reviewed by the DPC at any time.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

There are a number of international standards applicable to e-commerce which also operate in Ireland.

PCI DSS (Payment Card Industry Data Security Standard)
This sets out a widely accepted international set of security controls that was established to help businesses safely process credit card, debit card, and cash card transactions. The standards are applicable to any businesses that store, process or transmit cardholder data.

Payment Services Regulations (S.I. No. 6/2018 - European Union (Payment Services) Regulations 2018)
This implemented the revised Payment Services Directive – Directive on payment services in the internal market (EU) 2015/2366.

For further details see question 11.1.

ISO 27001/27002 (International Organization for Standardization)
This sets out the specification for an information security management system. This is seen as the 'gold standard'. Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology. It is mostly for large organisations, and was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

The Criminal Justice (Offences Relating to Information Systems) Act 2017
This piece of legislation sets out essentially five types of hacking or cyber-crime offences. These are:

- accessing an information system without lawful authority;
- interference with an information system without lawful authority;
- interference with data without lawful authority;
- intercepting the transmission of data without lawful authority; and
- use of a computer program, password, code or data for any of the above.

The GDPR/Data Protection Act 2018
The Data Protection Act 2018 implemented the GDPR in Ireland and governs how personal data is collected in Ireland. It requires that businesses keep personal data secure and only permit third parties' access to personal data subject to sufficient guarantees regarding the security of the processing services. Businesses must implement measures that are both technical (e.g., firewalls, anti-virus programs, perimeter scanning tools) and organisational (e.g., policies and procedures that must be followed by personnel regarding cybersecurity) to safeguard personal data. Businesses are required to protect against unauthorised or unlawful use of personal data and against loss, destruction and damage of the same.

Article 32 GDPR (section 72 DPA) requires controllers and processors to implement technical and organisational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data.

The e-Privacy Regulations (S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011)
The e-Privacy Regulations govern the use electronic communications. In particular they set out the rules applicable to marketing emails, texts and phone calls; they also govern the use of cookies; however, note that the consent required for the use

© Published and reproduced with kind permission by Global Legal Group Ltd, London

of cookies has now changed to a GDPR standard (see question 2.1 above). In addition, they also cover the security of public electronic communications services and data privacy.

A new EU e-Privacy Regulation has been under discussion for a number of years now, but at the time of writing is still in draft form. It will be broader in scope that the current regime applying not only to traditional telecommunications operators but all communications service providers including instant messaging apps and the like.

The NISD Regulations (the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018)

The NISD Regulations implement the Security of Network and Information Systems Directive 2016/1148/EU in Ireland. That Directive sets out to harmonise cybersecurity measures for operators of "essential services" (such as businesses in the energy, transport and/or health sector) and "digital service providers" (such as cloud service providers and providers of online marketplaces) that offer services to individuals.

Businesses subject to the NISD Regulations are required to implement appropriate and proportionate measures to manage risks posed to network and information systems and to prevent, and minimise the impact of, incidents affecting the security of the network and information systems.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

In general, Irish people have embraced new technologies and the numbers shopping online continue to grow. In PricewaterhouseCoopers (PWC) "Irish Retail and Consumer Report for 2019", they note that one in five Irish people shop at least once weekly from their mobile phone, a figure that has doubled over a two-year period.

While this number was expected to grow anyway in 2020, the arrival of the COVID-19 pandemic in Ireland has seen online shopping in general soar to new heights. Indeed, IBIS World reports that between 30 March and 5 April 2020 alone, internet-based sales in Ireland increased by 19%.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Ireland has a relatively young population which adapts quickly to change and new opportunities. While cash may have been key for the older generation, even most of those have become comfortable with the use of cards.

In PWC's Report, it is stated that 16% of all Irish consumers used their mobile device to make payments in 2018. This is expected to grow to 22% over the next 12 months against a global average of 34%. The growth of mobile payments is being most rapidly adopted by young millennials, more than 32% of whom expect to use the technology this year.

However, the J.P. Morgan "2019 Payments Trends – Global Insights Report" says that 52% of Irish consumers are concerned about security when making mobile payments.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

The J.P. Morgan Report notes the willingness of Irish shoppers to purchase from abroad. In fact, Ireland has the highest percentage of "cross-border" shoppers in Western Europe, with 84% of online shoppers making purchases from abroad. Foreign purchases are estimated to account for at least 23% of all online sales in Ireland.

While there is a great enthusiasm to buy Irish, domestic retailers have been criticised for being too slow to make their websites transactional. Only 32% of SMEs have transactional websites.

In April 2020, a scheme was introduced to assist traders. Administered by Enterprise Ireland, the state agency, retailers can now avail of grants up to €40,000 to help them develop their online trading capacity.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Ireland has a huge technology base with many of the world's largest technology and social media companies having their EMEA headquarters or manufacturing facilities here. So, it is no surprise therefore that companies such as Apple and Microsoft are among Ireland's biggest exporters.

Some well-known indigenous brands which would be seen as "typically Irish", such as Waterford Crystal, have been very successful in selling abroad and trade substantially through their websites. Another successful growth area is clothes. Magee, an Irish suit maker, saw an 80% growth in foreign online sales after re-purposing its website.

Enterprise Ireland assists companies in their drive into global markets.

It is estimated that nearly 52% of Irish exports go to Europe, 32% to the United States and 11.4% to Asia.

Language is not seen as a barrier as most Europeans in particular have English as a second language.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

There are no particular trends that are peculiar to Ireland. All website operators are encouraged to make navigation simple and their websites must be mobile-friendly. Of the top 10 most popular websites in Ireland, only two belong to Irish companies.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

There are a number of pieces of legislation that can be used to protect brands and prosecute offenders.

Trademarks

These can be registered in Ireland or in the European Intellectual

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Property Office, or the World Intellectual Property Office depending on the international scope of protection required.

Actions for infringement can be brought by the trademark owner under the Trade Marks Act 1996, or the EU Trademark Regulation (Regulation (EC) 207/2009) for EIPO trademarks.

The Director of Public Prosecutions can also initiate criminal proceedings under the Trade Marks Act 1996 for trademark infringement.

Unregistered trademarks can be protected by taking an action for passing off, which is a common law tort – where one party attempts to mislead the public into thinking that their brand is associated with another brand.

Copyright

Copyright is protected in Irish law by the Copyright and Related Rights Act, 2000 (CRRA). Protection is automatic and there is no system of registration in Ireland.

Subject to some small fair dealing exceptions, a copyright owner can prevent another party from using its work without permission (usually granted by way of a licence for a royalty). A copyright owner can sue for infringement under the CRRA.

Domain Names

These are now a crucial part of a company's branding. The most common issues are firstly cyber-squatting, where someone registers a name to thwart a genuine user's ability to register it in the hope of extracting a large price for it; the second is where different companies may have legitimate interests in the same domain name.

Under ICANN rules, an aggrieved trademark holder can use the Uniform Domain Name Dispute Resolution Policy to try and resolve these issues.

Designs

For infringement of design rights in the EU, an injured party can avail of the regime under the European Community Designs Regulation (6/2002/EC) (CDR). The CDR is augmented by EIPO guidelines issued from time to time.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Ireland does not have a separate court for intellectual property litigation, and instead such disputes go through the regular court system.

Litigation in Ireland tends to be an expensive undertaking, especially in the higher courts and many digital businesses are early stage companies, which may not have the resources to fund a long court case. Alternative dispute mechanisms are available in Ireland and many such companies now seek to use these.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

If a company is using the infrastructure located in a data centre to run its business or contracting with a cloud services provider for that purpose, then it will need to ensure its data will remain secure, available and accessible. This is typically done through a services agreement, which should contain a commitment to those matters as well as to service levels.

If a company is a controller of personal data, then it will be required to include a data processing agreement or addendum as part of its contractual arrangements with the service provider, to meet its obligations under Article 28 of the GDPR (section 80 DPA).

The DPC has published guidance on its website as to what conditions they consider to be mandatory for such contracts.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

There are none. However, a controller is subject to Chapter 5 of the GDPR, which governs transfers of personal data to third countries and international organisations. Article 44 of the GDPR (and a number of sections of the DPA) states that if a controller transfers personal data out of the EU, it must enjoy the same level of protection as it gets under the GDPR.

In the absence of an adequacy decision or consent, personal data may still be transferred to a non-EEA country subject to the putting in place one of the appropriate safeguards set out in Article 46 of the GDPR (section 98 DPA). These include the "Standard Contractual Clauses" or "Binding Corporate Rules". The safeguards must be outlined in a legally binding contract between the transferring and recipient parties.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

In 2017, Ireland adopted a new trade and investment strategy, "Ireland Connected: Trading and Investing in a Dynamic World". Part of that strategy includes "connectedness" and the harnessing of digital technologies to increase and facilitate trade.

Irish Revenue and Customs already only use automated processes for interacting with traders importing goods into Ireland, and in November 2020 and March 2021, will substantially upgrade those improving trade facilitation further.

Going forward for Ireland, much of the discussion has revolved around Brexit and how technology could be used to implement a seamless border between Northern Ireland and the Republic (the only EU land border with the UK).

In the absence of a trade agreement between the EU and the UK, goods coming into Ireland from the UK will have to be checked for compliance with EU standards, tariffs and places of origin.

In this context paperless trading, registration of information online and e-certificates are all being examined.

In March 2020, "The Spectator" magazine reported that the British government was in talks with Fujitsu to create a "drive through border" using their technology.

However, so far in May 2020, no one has put forward a technical solution which the Irish or EU authorities believe could fully replace physical checks at or near the border.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

While digital technologies for trade in general, such as those used by the Irish Revenue and Customs Service, will no doubt

© Published and reproduced with kind permission by Global Legal Group Ltd, London

continue to develop and the WTO and OECD are very active in this area, the Northern Ireland border is still likely to be an issue for some time to come in the event of a no-deal Brexit.

While many solutions have been promulgated in general terms, none of the stakeholders have so far come up with a technology solution that all parties can agree as workable.

Even if one can be found it could involve the EU and UK having to share highly integrated systems in respect of VAT and the like, and that may not be possible without an over-riding trade agreement.

Even Norway, whose trade systems with its neighbours are put forward by some as a solution to the Irish border problem, is not allowed full access to the EU VAT system.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Ireland has a number of tax incentives which are available to digital businesses.

There is a 25% tax credit available to companies for research and development expenditure. This can be claimed for activity prior to trading also. The credit can be offset against the company's corporation tax liability in the year in which it occurred. It can be claimed in addition to a 12.5% deduction for the expenditure, giving an effective rate of 37.5%.

The tax legislation also provides for a tax deduction for trading companies which expend capital on qualifying intellectual property assets. They are defined quite broadly and include patents, trademarks, copyright goodwill, domain names and customer lists.

The Knowledge Development Box provides for a lower corporation tax rate of 6.25% on profits arising from qualifying assets, which are themselves the product of qualifying R&D. This incentive is fully compliant with the OECD's modified nexus approach (linking the relief to R&D and IP). To avail of the relief, a company must be earning income from those qualifying assets (such as through licensing or other exploitation).

Under the Taxes Consolidation Act 1997 (as updated each year by the Finance Act), there is also currently a tax relief available for start-up companies up to 2021 with corporation tax due of €40,000 or less in a tax year (and partial relief if it is between €40,000 and €60,000). The exact amount of the relief will depend on the number of employees in the company.

Acquisitions of IP are also exempt from stamp duty in Ireland.

There are additional grants and services made available through the IDA (Ireland's agency for inward investment) to foreign companies who are considering investing in Ireland.

Finally, Ireland has a low corporate tax rate of 12.5% which makes it attractive for companies to locate here.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

VAT would seem the most likely area where disputes will arise for a number of reasons.

VAT distinguishes between goods and services (services being everything that is not a good!). In the world of digital and downloads, the distinction may become more difficult (which is important in terms of determining place of supply and accountability).

From 2021, there will be changes to how the current tax thresholds for B2C will operate. Currently, a B2C online trader can apply VAT in its home country on its distance sales of goods until the point that they exceed the relevant threshold in the customer's EU Member State. From 2021, the individual thresholds in each Member State will be replaced by a single EU-wide threshold of €10,000. Thereafter, once the trader has achieved those sales across the whole of the EU, it will be forced to apply the rate applicable in the customer's home country. This will require knowledge of all the different VAT rates applicable in the different Member States. This is by no means a simple task and may lead to miscalculations and disputes.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

In Ireland, individuals are either employees or self-employed, independent contractors; there is no intermediate or hybrid status. How the relationship is described in the written agreement between the parties is only one of a number of factors that will be taken in to account when determining whether an individual is an employee or an independent contractor; what is important is how the relationship works in practice. The level of "control" exercised by a company over an individual and their work is the most common factor used to determine whether someone is an employee or not. A company should consider how the arrangement works in practice and should ensure that the written agreement accurately reflects this.

The vast majority of employment rights are afforded to employees only, for example, the right to be paid for annual leave and minimum wage, protection from unfair dismissal and the right to a redundancy payment. Both employees and independent contractors will benefit from the protections afforded by whistleblowing and equality legislation. Independent contractor arrangements work best where the individual is in business on their own account and they provide services to more than one client. This type of agreement provides flexibility to both parties and can be advantageous from a tax perspective as no employer PRSI (social insurance) is payable. However, mis-classifying an individual as self-employed when in reality they are an employee could result in significant costs for a company which will be liable for any underpayment of tax and social security plus interests and penalties. It also means that the individual will have accrued statutory employment law rights as against that company.

There are a number of different types of employment arrangements, depending on what type of resourcing a company requires. For example, a company may want to employ individuals on a part-time basis or for a specific project or fixed duration. Alternatively, companies may choose to engage an employment agency to supply staff, rather than hire them directly. Irish employment law generally does not distinguish between these different categories of employees and there is much legislation in place to ensure that these categories of employees are treated no less favourably than permanent, full-time employees. "Zero-hour" contracts which require individuals to be available for work but with no guaranteed hours are prohibited by the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Employment (Miscellaneous Provisions) Act 2018 except for in very limited circumstances.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

A company has obligations under employment law in respect of all its employees, whether they carry out work on or away from its physical premises. While there is no specific regulation in place in Ireland which regulates remote working, employers should pay particular regard to their obligations under health and safety, working time and data protection legislation.

Under the Safety, Health and Welfare at Work Act 2005, employers have specific duties to ensure the safety, health and welfare at work of all employees, whether or not that work is being done at the employer's premises. This includes providing and maintaining a safe workplace, preventing any improper conduct or behaviour likely to put the safety, health and welfare of employees at risk and providing instruction and training to employees on health and safety. Employers must carry out a risk assessment of the work-place, even where this is not the employer's premises (for example, an employee's home office). Organisations should have policies in place which clearly set out the employer's and employees' health and safety obligations including an obligation on employees to report health and safety risks and work-related accidents.

The Organisation of Working Time Act 1997 governs minimum working hours and rest breaks. Under the Act, employers are obliged to record employees' working time on a daily basis including start and finish times and rest breaks. Remote working can make it particularly challenging for organisations to comply with their working time obligations. Employers should put in place policies and systems for recording employees' working hours and rest breaks when working away from their premises.

Compliance with the GDPR/DPA will also be an issue where employees are not based at a company's premises. Companies should put in place robust data protection policies including procedures for reporting data breaches and ensure ongoing training for all staff on their data protection obligations. Extra security measures may need to be taken for employees working remotely, such as the provision of encrypted laptops.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

There are no real legal barriers to entry, such as registration for example, but there is much legislation and regulation to deal with as set out elsewhere in this chapter.

A B2B offering will of course be easier to set up and mange than a B2C offering, as the trader will not have to deal with consumer legislation.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

There are considerable advantages for a digital business operating in Ireland.

In section 8, the various tax incentives are described, as well as the grants available from the IDA for foreign companies setting up in Ireland.

In addition, we have a well-educated and trained workforce able to work easily in the technology industry generally.

Ireland is strategically situated between Europe the UK and the United States.

At the end of 2020, it will be the only English-speaking country in the EU.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Payment Services Regulations 2018 (S.I. No. 6/2018 - European Union (Payment Services) Regulations 2018 (PSR)

These implemented the revised Payment Services Directive (EU) 2015/2366 – PSD2) and replaced the 2009 Regulations (PSD1). They are the most important piece of legislation in respect of online payments.

The PSR are intended to reduce fraud while opening up payment markets to new entrants. Their operation in Ireland is governed by the Central Bank of Ireland (CBI).

PSD2 is intended to be a positive development for all users of payment services, but particularly consumers. It introduced the concept of Strong Customer Authentication.

For the purposes of reducing fraud, the CBI has set a deadline of 31 December 2020 for compliance with SCA for electronic commerce card-based payment transactions.

E-Money Regulations (the European Communities (Electronic Money) Regulations 2011)

The E-Money Regulations transposed Directive 2009/110/EC into Irish law and apply to providers of e-money services. The E-Money Regulations have been further updated by PSD2.

The GDPR/Data Protection Act 2018

This will also be applicable to online payment service providers. For more detailed analysis, see elsewhere in this chapter.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Online payment providers must comply with the provisions of PSD2 as described in question 11.1. This will involve initially an authorisation and approval process carried out by the CBI, before any service can begin.

An authorisation process is also required for e-money service providers under the E-Money Regulations.

PSD2 and the E-Money Regulations set out various capital and probity measures which a company must meet in order to be authorised.

The CBI places much emphasis on having "hearts and minds" located in Ireland. This essentially means that the CBI will need to be satisfied that the applicant will be properly run in Ireland and that the CBI will be able to supervise it effectively. As a minimum, it requires a senior management team overseen by a strong board and an appropriate organisation structure with reporting lines.

Online payment providers will also need to be mindful of the GDPR and where applicable consumer legislation, described elsewhere in this chapter. In addition, the CBI has published a number of consumer codes which may be relevant.

Finally, they may also be subject to anti-money laundering legislation.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Victor Timon is a partner in the Dublin office of the international law firm Lewis Silkin, where he heads up the Commercial, Technology and Data practice of the firm.
He has over 35 years of legal experience having been an in-house counsel and then a partner in leading law firms in London and Dublin.
Victor is qualified to practice in both England and Ireland.
He regularly speaks at conferences on e-commerce, technology and data privacy issues in particular.
Victor is a member of ITechLaw, the global association for technology lawyers which spans more than 60 countries and helped organise their European Conference in Dublin in 2019.

Lewis Silkin
26 Lower Baggot Street
Dublin 2
Ireland

Tel: +353 1566 4508
Email: victor.timon@lewissilkin.com
URL: www.lewissilkin.com

In a world full of possibilities, we help make the most of what really matters to you – your Ideas, your People, your Future. We pride ourselves on providing solutions to your most complex business challenges, with a pragmatic and human touch.
We have renowned expertise advising creative, innovative and tech-focused businesses across all sectors and our multi-disciplinary teams provide clients with commercial insight and specialist knowledge from a range of legal disciplines including: commercial; IP; data and privacy; corporate; employment; immigration; dispute resolution; and real estate.
We work with an international community of clients, helping them achieve their business objectives worldwide through a combination of our own offices, international desks and strategic alliances.
Our people are at the heart of what we do, and are committed to building strong, long-lasting relationships, to providing efficient, high-quality and cost-effective legal services, and to constantly challenge ourselves to provide creative solutions.

www.lewissilkin.com

LEWIS SILKIN

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms
Workplace Pensions

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group