International Comparative Legal Guides

Digital Business 2026

A practical cross-border resource to inform legal minds

Seventh Edition

Contributing Editor:
James Gill
Lewis Silkin LLP

glg Global Legal Group

iclg

Expert Analysis Chapter

Q&A Chapters

United Kingdom

Littleton Chambers

Andrew Maguire

1 E-Commerce Regulation

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 with regulatory bodies, as well as a summary of legal obligations specific to B2B e-commerce.

B2B e-commerce is subject to the following legal obligations, for online business:

1. The Company, Limited Liability Partnership and Business (Names and Trading Disclosures) Regulations 2015 require that companies and LLPs disclose certain information on their website and e-business communications and forms, such as their registered name and email disclaimers.
2. Information Society Service Providers (which includes businesses self-hosting e-commerce websites and online market platforms) are required to comply with the Electronic Commerce (EC Directive) Regulations 2002; the main requirements being pre-contractual information as to identity and making information about promotions "easily accessible and presented clearly and unambiguously", which must be provided.
3. The Assimilated Regulation (EU) 2019/1150 is the UK's Platform-to-Business Regulation and protects businesses against market abuse by large online platforms by promoting fairness and transparency.
4. The parties are obliged to comply with the UK's data protection laws, regarding personal data in connection with any data processing in any e-commerce transaction, which are contained in the General Data Protection Regulation 2016/679 (known as the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018").
5. Cybersecurity is a key consideration for e-commerce businesses and the UK statutory framework introduces workable security requirements on operators of essential services ("OESs") and certain digital service providers ("DSPs") through the Network and Information Systems Regulations 2018 ("NIS Regulations"). A new Cyber Security and Resilience Act 2025 is anticipated, which will cover digital services, such as online marketplaces, online search engines, and cloud computing services.
6. Misleading marketing and advertising is prohibited through the Business Protection from Misleading Marketing Regulations 2008, which applies to e-commerce.
7. Limitations and exclusions of liability are governed by the "reasonableness" test as laid down by the Unfair Contract Terms Act 1977, which applies to e-commerce B2B.
8. Financial services e-business is regulated by the Financial Services and Markets Act 2000, as amended ("FSMA"), and the Financial Conduct Authority ("FCA") Guidebook. The financial promotion of cryptocurrency transactions is a regulated activity, which requires registration with the FCA and its "fit and proper person" regime.
9. An e-commerce business, if a limited liability company or LLP, will need to be incorporated and be registered at Companies House and HM Revenue and Customs ("HMRC") for tax purposes, including for Value Added Tax ("VAT") if over a certain income threshold.

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 with regulatory bodies, as well as a summary of legal obligations specific to B2C e-commerce.

Consumers are protected by the requirements set out in question 1.1 above. In addition, B2C e-commerce businesses are required to adhere to the following legal requirements:

1. The Unfair Contract Terms Act 1977 has greater force when a consumer is a contracting party.
2. The Consumer Credit Act 1974, as amended by the Consumer Credit Act 2006, contains an extensive code designed to protect the interests of consumers and, for the first time, introduces an "Unfair Relationship", which introduces the concept of good faith to sit alongside the traditional *caveat emptor* or "buyer beware" hallmark of English contract law.
3. The Consumer Rights Act 2015 introduced a streamlined system to make redress easier for consumers and introduced specific rights for digital content, including rights related to quality, fitness, and description.
4. The Online Safety Act 2023 is a statutory law designed at making internet services safer for users; in particular, children. It places new duties on online service providers, including social media companies and e-business search engines, to take action against illegal content and harmful material.

1.3 Please explain briefly how the EU's Digital Services Act and Digital Markets Act and/or equivalent local legislation, such as the UK's Online Safety Act and Digital Markets, Competition and Consumers Act, are affecting digital business in your jurisdiction.

The Digital Markets, Competition and Consumers Act 2024, which primarily came into force on 1 January 2025, and latterly 6 April 2025, and amends: (i) the Consumer Protection from Unfair Trading Regulations 2008; (ii) the Competition Act 1998; and (iii) the Enterprise Act 2002. Its main provisions are:

1. The 2024 Act creates a new regime to increase competition in digital markets.
2. It provides the Competition and Markets Authority ("CMA") with enhanced powers to regulate competition in digital markets and to directly enforce consumer law.
3. Part 1 of the 2024 Act provides for:
   i. the designation of undertakings as having strategic market status in respect of a digital activity;
   ii. the CMA being given powers to impose conduct requirements on a designated undertaking and to take steps to promote competition through pro-competition interventions where it finds an adverse effect on competition in respect of a designated activity;
   iii. the introduction of a duty to report possible mergers involving a designated undertaking or its corporate group;
   iv. the introduction of a series of investigatory powers and requirements to produce compliance reports in respect of a designated activity; and
   v. enforcement, appeals and administrative matters relating to the CMA's powers and duties under the digital markets regime.
4. Part 2 of the 2024 Act provides for:
   i. the amending of powers to investigate and enforce against suspected infringements of the Competition Act 1998 Chapter I and II prohibitions;
   ii. making changes to the Enterprise Act 2002 merger jurisdictional thresholds, as well as providing for some procedural changes to merger reviews;
   iii. making changes to the Enterprise Act 2002 to introduce a new regime to prevent foreign state control or influence over newspapers and periodic news magazines;
   iv. making changes to the procedures for market studies and investigations under the Enterprise Act 2002, including provision for a new power to conduct trials of certain remedies to determine their final format;
   v. amending the CMA's power to require the production of information held electronically and accessible from a premises when acting under a warrant during an investigation (section 192 of the Enterprise Act 2002); and
   vi. miscellaneous provisions, including with regard to civil penalties and the extra-territorial reach of information notices in connection with competition matters.
5. Part 4 of the 2024 Act prohibits unfair commercial practices; in particular:
   i. it replaces and updates the Consumer Protection from Unfair Trading Regulations 2008;
   ii. it prohibits the "drip pricing" of unavoidable fees by requiring traders to set out in an invitation to purchase the total price of a product including any mandatory fees, taxes and charges that apply to the purchase of a product;
   iii. it adds a banned practice relating to fake consumer reviews to the Schedule 20 list of commercial practices, which are in all circumstances considered unfair;
   iv. it imposes duties on traders in relation to subscription contracts, provides rights for consumers if those duties are breached and provides rights for consumers to cancel subscription contracts during cooling-off periods;
   v. it gives protections to consumers in respect of payments to consumer savings scheme contracts; and
   vi. it prohibits alternative dispute resolution procedures for consumer contracts where the provider is not accredited nor exempt and makes provision for accreditation and exemption, related requirements and enforcement.
6. The Online Safety Act 2023 was introduced to make online services safer for users: it makes provision for and in connection with the regulation by Ofcom of certain internet services for and in connection with communications offences and for connected purposes. It provides for:
   i. the establishment of a new regulatory regime to address illegal and harmful content online;
   ii. imposing legal requirements on: (a) providers of internet services that allow users to encounter content generated, uploaded or shared by other users (user-to-user services); and (b) the provision of search engines that enable users to search multiple websites and databases (search services); and
   iii. the conferring of new powers on Ofcom, enabling it to act as the online safety regulator. This role will include overseeing and enforcing the new regulatory regime.

1.4 Are there are any new laws planned in your jurisdiction that will affect e-commerce going forward?

Yes, the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 ("Cryptoasset Regulations") establish a regulatory regime for certain cryptoasset activities pursuant to powers conferred by the FSMA. Part 1 of the Cryptoasset Regulations provides that some provisions commenced early to enable the FCA to give directions or guidance, make rules and carry out preparatory steps, with most remaining provisions coming into force on 25 October 2027.

Part 2 of the Cryptoasset Regulations introduces two designated activity regimes under Part 5A of the FSMA: the first for public offers of qualifying cryptoassets and admissions to trading on qualifying cryptoasset trading platforms; and the second covering market abuse including insider dealing, disclosure of inside information and market manipulation.

Part 3 of the Cryptoasset Regulations amends the Financial Services and Markets Act 2000 (Regulated Activities Order) 2001, as amended ("RAO") to include the definition of qualifying cryptoassets in a new article 88F, as a subcategory of cryptoassets that are fungible and transferable. Excluded from this definition are tokenised versions of existing specified investments, records of value or contractual rights, and other instruments that could meet the definition of a cryptoasset under the FSMA such as tokenised e-money or tokenised deposits, which are already subject to regulation.

Part 6 of the Cryptoasset Regulations makes consequential amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs 2017") to account for the relevant new regulated activities created by the Regulations. Firms that become authorised for the new cryptoasset regulated activities will

not need to additionally register as cryptoasset exchange providers or custodian wallet providers under the MLRs 2017. The FCA will be required to maintain a register of cryptoasset exchange providers and custodian wallet providers that are not authorised cryptoasset firms.

HM Treasury expects firms undertaking regulated cryptoasset activities under the new regime to comply with the same financial crime standards and rules under the FSMA that apply to equivalent or similar traditional financial services activities. This means that other than the requirement to register, the existing requirements of the MLRs 2017 will continue to apply to these authorised firms in full.

The Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) Order 2001 was amended to include, as investment business: article 9M (issuing qualifying stablecoin); article 9N (safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets); article 9S (operating a qualifying cryptoasset trading platform); article 9T (dealing in qualifying cryptoassets as principal); article 9W (dealing in qualifying cryptoassets as agent); article 9Y (arranging deals in qualifying cryptoassets); and article 9Z6 (qualifying cryptoasset staking).

2 Data Protection

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

Data protection law has been developed over the recent years in the UK as follows:

1. The Data Protection and Digital Information Bill was first introduced during the 2022–23 parliamentary session. It did not complete before Parliament was dissolved on 24 May 2024, and is no longer being progressed.
2. In its place, the new Government introduced the Data (Use and Access) Bill, which was introduced to Parliament on 24 October 2024. The Bill has now completed its passage through the House of Lords, where it has been subject to a number of amendments and significant debate.
3. It has been heralded as a positive package of reform that maintains high standards of data protection and protects people's rights and freedom; its core objectives being to help grow the economy, improve UK public services, and make people's lives easier – it also seeks to provide greater regulatory certainty for organisations and promotes growth and innovation in the UK economy.
4. The Bill will provide the following:
   i. the Office for Digital Identities and Attributes ("OfDIA") will oversee a standards framework for online digital verification services; and
   ii. the creation of a "smart data" regime, introducing separate smart data schemes to address specific sector needs, such as in finance, telecoms and energy. Such smart data schemes will allow individuals to request that their data be shared directly with them, as well as with authorised third parties, and launch a supporting framework to guarantee the secure storage and transfer of such data.
5. The Bill provides that certain types of processing purposes will be more likely to count as legitimate interests, including processing for the purposes of: (i) direct marketing; (ii) intra-group transfers for internal administration; and (iii) network and IT system security. It is proposed that this should make it much easier for e-commerce businesses to use the legitimate interest ground is the basis for processing in these areas.

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

Anti-Money Laundering ("AML") measures may generally be improved by AI; however, some specific problems persist, such as:

i. some AI-powered security measures do not directly identify questionable activities: the aim being to consistently allocate risk levels to disparate transactions;
ii. accurately incorporating past transaction data into AI-driven pricing recommendations while ensuring compliance with data security regulations.
iii. predicting market shifts and adjusting strategies without introducing bias or inaccuracies;
iv. data-driven pricing needing to be constantly updated, and accurate and complete; the need to ensure that AI tools provided by commercial operators can be properly used with current systems; and
v. the continuous threat of, and need to prevent, sophisticated cyberattacks, such as compromised AI systems being subject to ransomware attacks.

2.3 What support are the government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health, such as, for example, sandboxes?

To support businesses developing new digital products in the area of AI, the FCA established the "Innovation Hub" (a unit within the FCA, pitched entirely to working with innovative businesses). The Innovation Hub offers support to innovator businesses that are looking to introduce ground-breaking or significantly different financial products or services to the market, including when they need assistance with an application for authorisation or a variation of permission. The services provided through the Innovation Hub include: (i) the Regulatory Sandbox; (ii) Innovation Pathways; (iii) the Digital Sandbox; (iv) RegTech; (v) the Global Finance Innovation Network ("GFIN"); and (vi) the Emerging Technology Research Hub.

On 22 April 2024, the FCA published a guidance update that outlined the regulator's approach to AI following the Government's publication of its pro-innovation strategy on AI. The FCA stated that it welcomed the Government's publication of "A Pro-Innovation Approach to AI Regulation: Government Response" and "Implementing the UK's AI Regulatory Principles: Initial Guidance for Regulators". The update also described what the FCA planned to do in the following 12 months. This included:

i. continuing to further the FCA's understanding of AI deployment in UK financial markets by continuing to build a thorough understanding of how AI is deployed in UK markets so as to seek to ensure that any potential future regulatory interventions are effective and yet proportionate and pro-innovation;
ii. building on existing foundations: the existing regulatory framework covers firms' use of technology, including AI;
iii. continuing to collaborate domestically and internationally with: the Bank of England; the Payments Systems Regulator; and other regulators through membership of the Digital Regulation Cooperation Forum ("DRCF");
iv. further prioritising its international engagement on AI, such as the International Organization of Securities Commissions, including the AI working group, and supporting the work of the Financial Stability Board, as well as being a core participant in other multilateral forums on AI, including the Organisation for Economic

Co-operation and Development ("OECD"), the GFIN and the Group of Seven ("G7");

v. testing for beneficial AI: this includes exploring changes to its innovation services that could enable the testing, design, governance and impact of AI technologies in UK financial markets within an AI Sandbox;

vi. the FCA's own use of AI, such as web scraping and social media tools that are able to detect, review and triage potential scam websites. The FCA is also exploring potential benefits involving Natural Language Processing to aid triage decisions, assessing AI to generate synthetic data or using LLMs to analyse and to summarise text; and

vii. the FCA declared that it took a proactive approach to understanding emerging technologies, and their potential impact, as a part of its Emerging Technology Research Hub. By way of example, within the DRCF Horizon Scanning & Emerging Technologies workstream in 2024–25, the FCA would conduct research on deep-fakes and simulated content following engagement with stakeholders.

3 Cybersecurity Framework

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

The National Cyber Security Centre ("NCSC"), on 28 April 2024, published a very helpful, comprehensive Cyber Assessment Framework ("CAF"), which repays reading. It provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. CAF-based assessments can be carried out either by the responsible organisation itself (self-assessment) or by an independent external entity, possibly a regulator/cyber oversight body or a suitably qualified organisation acting on behalf of a regulator, such as an NCSC-assured commercial service provider.

The NCSC CAF cybersecurity and resilience objectives and principles provide the foundations of the CAF. The four high-level objectives (A–D) and the 14 principles laid out within the CAF collection are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The CAF adds additional levels of detail to the top-level principles, including a collection of structured sets of Indicators of Good Practice ("IGPs").

Other relevant cybersecurity frameworks are provided by the UK GDPR, and the NIS Regulations, as referred to above. App Store Operators and Developers must adhere to their legal obligations under data protection law at all times, including on when and how to inform data subjects and the supervisory authority about a data breach (UK GDPR).

There is also a voluntary Code of Practice for App Store Operators and App Developers published by the Department for Science, Innovation and Technology, which prescribes mandatory, minimum security and privacy requirements.

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

The Computer Misuse Act 1990 is the main cybersecurity act that regulates the UK's digital relationship between individuals and malicious parties. It is enforced directly with the DPA 2018 and the UK GDPR, which protect UK residents' personal data.

In addition, recourse may be had to: (i) the NIS Regulations (these Regulations place security duties on OESs to safeguard the cyber and physical resilience of critical infrastructure); (ii) the Online Safety Act 2023, which requires online platforms to take action against illegal content and activity, including implementing measures to reduce risks and remove illegal content; (iii) the Telecommunications (Security) Act 2021, which strengthens cybersecurity for the telecommunications sector, including measures to ensure the security of critical infrastructure; and (iv) the forthcoming Cyber Security and Resilience Bill, yet to be enacted, which aims to further strengthen the UK's cybersecurity framework and protect critical infrastructure.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or do consumers still prefer shopping in person?

Consumers in the UK have wholeheartedly embraced e-commerce. According to the research organisation, Statista: "*The United Kingdom boasts the most developed e-commerce market in Europe. The e-commerce penetration rate on the British isles is nearing the 85 percent mark in 2025. For context, the European average is just under 50 percent, meaning that while less than half of all Europeans shop online, nearly all UK consumers do. Further e-commerce growth in the United Kingdom is dependent on how merchants, retailers, and logistics companies listen to consumer preferences, from product discovery to payment and delivery.*"[1,2]

The UK Office for National Statistics has reported that more than one in six (18%) of businesses reported that they are currently using some form of AI technology in late March 2025, broadly stable with late December 2024, but up eight percentage points since the question was first introduced in late September 2023; for businesses with 250 employees or more, this increased to 31%, up 13 percentage points compared to September 2023.

In addition, when asked in late March 2025, 77% of businesses reported they were not planning to adopt AI technologies in the next three months, down three percentage points since late December 2024; the transportation and storage and construction industries had the largest proportion of businesses to report this, at 87% and 86%, respectively.

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?

In the UK, there is a strong debit card culture and a widely accepted direct debit culture, while cash on delivery ("COD") is less prevalent. Debit cards are the most common payment method, especially for physical transactions, followed by credit cards and then cash. Direct debits are also very popular for recurring payments like bills.

In 2024, the Labour Party (then) in opposition (now in Government) published a working paper: "Financing Growth", which stated that it intended to "*[e]mbrace innovation and fintech as the future of financial services by becoming a global standard-setter for the use of AI in FS, delivering the next phase of Open Banking, defining a roadmap for Open Finance, embracing securities tokenisation and a central bank digital currency, and establishing a regulatory sandbox for financial products to reach underserved communities*".

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

According to Statista, global retail e-commerce sales are projected to exceed $8 trillion by 2027, a huge leap from $2.3 trillion in 2017. The UK is said to rank third globally, behind the USA and China, with sales projected to reach $220 billion, reflecting a steady annual growth of 5.3%.

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?

Statista predicted that cross-border e-commerce would account for 22% of all e-commerce shipments by 2025.

Furthermore, a 2023 study by Accenture found that over 57% of online shoppers have purchased from an overseas retailer.[3]

Expanding into international markets requires businesses to navigate language and cultural barriers. Companies need to localise websites, product descriptions, and marketing materials to resonate with customers in different countries. Additionally, providing customer support in multiple languages is crucial for building trust and ensuring a positive shopping experience.

Language switcher tools are a simple yet effective way to cater to a global audience. These tools allow users to switch between different languages on your website, making it easier for them to navigate and understand your content.

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

User interface design in e-commerce is regulated in the UK by the applicable equality laws as found in the Equality Act 2010 – ensuring accessibility to all is underpinned by reasonable adjustments being required.

The DRCF was established as a voluntary forum in 2020. It brings together four UK regulators with responsibilities for digital regulation – the CMA, the FCA, the Information Commissioner's Office ("ICO") and Ofcom.

The DRFC have recently published a series of case studies based on informal advice from the AI and Digital Hub. These case studies enable more innovators and businesses to benefit from the advice generated through the Hub.

The case studies map out how current regulation within DRCF's members' remits applies in innovative situations. The examples will include: data protection and consumer law for businesses supporting SMEs to deploy AI; advertising financial promotions; and managing the impact of third-party software defeats on resilience.

The Hub is a one-stop shop for innovators to obtain free informal advice from all four DRCF member regulators – saving innovators time and money in bringing their products and services to market.

Its recent survey of 500 business leaders from digital and AI startups and small businesses showed that over eight in 10 (82%) agree regulatory compliance has helped their business innovate and grow responsibly. 85% of respondents said utilising regulatory guidance has been instrumental in building trust, managing risks and identifying new growth opportunities.

As the pioneer in digital regulatory cooperation, the DRCF is seen as a model internationally and we work actively with other countries in considering how to increase collaboration between regulatory authorities. In 2023, the DRFC launched the International Network for Digital Regulation Cooperation[4] ("INDRC") to link together overseas counterparts and share best practice on effective interdisciplinary cooperation.

4.6 Has the COVID-19 pandemic had any lasting impact on these cultural norms?

The COVID-19 pandemic naturally resulted in e-commerce's exponential increase in market share, which understandably lessened as restrictions were lifted. Nonetheless, as stated above, the UK market is the market leader in Europe for e-commerce, especially amongst the younger generations.

The enduring, long-term effects of the pandemic and the economic slowdown have resulted in some former "high street" businesses moving to online-only sales and some being incorporated via their acquiring successors' websites.

5 Brand Enforcement Online

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

Online brand enforcement in the UK involves identifying and addressing unauthorised uses of a brand online, often through monitoring, takedown requests, and the threat of legal action. This process includes monitoring for trademark infringements, counterfeit products, and other unauthorised uses of a brand's name, logo, or other intellectual property rights ("IPR") in their online brand and design.

Business that are affected may report IPR crime to: (i) their local authority's Trading Standards departments, who are responsible for enforcing IPR breaches in the UK; (ii) the Police's Intellectual Property Crime Unit; or (iii) Action Fraud. Many of the global e-commerce stores have developed specific tools to allow IPR holders to report and remove infringing listings to protect their brands.

The UK Government's Intellectual Property Office, in March 2025, published an updated, helpful guidance note titled: "Protecting Intellectual Property Rights on e-commerce stores", which provides details of where and who to complain to when copyright and IPR are breached by rogue operators.

In addition, it has updated its guidance contained in "Intellectual property: Crime and infringement", which is a collection of guidance about how to protect and enforce businesses' IPR, including information on infringement, counterfeiting and piracy.

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

No substantive restrictions exist in the UK's brand and design protection laws; they are considered by most to be in alignment with leading IPR protection as found in the USA and the EU.

The UK Government is very keen to ensure a robust regime as set out in the "IP Counter-Infringement Strategy 2022 to 2027", which outlines its commitment to addressing intellectual property infringement and counterfeiting. The Government's

efforts are driven by the understanding that intellectual property crime is a serious issue that can have significant economic and social consequences. By strengthening the UK's legal framework, collaborating with stakeholders, and raising public awareness, the UK Government aims to create a more secure and innovative environment for businesses and creators.

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?

When contracting with third-party data centres or cloud providers in the UK, the key legal considerations centre around: (i) data protection via the UK GDPR; (ii) IPR; (iii) service level agreements; (iv) liability for service failures; and (v) data location.

Specific risks to look out for include: (i) security breaches; (ii) data loss; (iii) compliance issues; and (iv) potential liability for data controller obligations, even if the customer does not have full control over the cloud environment, of which providers' exclusion or limitation clauses will need to be carefully scrutinised and considered prior to entering into a service level agreement.

Such data centre outsourcing introduces data protection issues, which must be key considerations.

The data protection regime in the UK is comprised of two main pieces of legislation: (i) the UK GDPR, a version of EU GDPR, Regulation (EU) 2016/679, which was incorporated into UK law at 11pm on 31 December 2020; and (ii) the DPA 2018, particularly the parts that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement.

Although the UK GDPR and the DPA 2018 should be read together, it is convenient to take the UK GDPR as the initial starting point and then consider the specific supplementary provisions of the DPA 2018, where necessary.

It may also be indispensable to consider the provisions of the EU GDPR where, for example, the personal data of EEA citizens is being processed for the purposes of offering those citizens goods or services. Thus, the UK GDPR and the EU GDPR remain closely aligned.

Plainly, customers of data centre services will need to ensure they comply (and that their supplier complies) with the applicable data protection regime. The UK GDPR distinguishes between controllers and processors. While processors have some direct statutory obligations under the UK GDPR, the contracting and compliance requirements differ depending on whether a party (or its counterpart) is a controller or processor. Customers should consider the encryption tools that the supplier uses. Encryption devices or methods may be subject to export controls in many countries.

These are issues that may require expert guidance prior to entering into a service level agreement. In particular, care will need to be taken to ensure that, amongst other matters, the following issues are adequately detailed in the service level agreement:

i. where the customer has access to or the use of software, to the extent that the supplier does not own the IPR in the software, it will need to arrange for the right to sub-license the software to the customer in all jurisdictions in which the customer operates;
ii. IPR indemnities for the customer's benefit for claims by third parties that use of the services by the customer infringes that third party's IPR, in all jurisdictions in which the software will be used or services accessed;
iii. an obligation on the supplier to notify the customer of any intended deletion or movement of data or material, and an indemnity for any loss suffered as a result of material being unnecessarily deleted or moved;
iv. appropriate confidentiality and data protection provisions;
v. consent or notification required for any assignment of the contract;
vi. the customer to have termination rights for change of control of the supplier; and
vii. the customer to have audit rights to ensure compliance with the agreement and any other certifications or standards; at the very least, require the supplier to provide a Service Organisation Control ("SOC 2") report on a regular basis.

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

No, companies are not required to use servers/data centres located in the UK.

If a company wishes to transfer data to an alternative jurisdiction, they must comply with all necessary UK GDPR obligations and mechanisms that permit such transfers.

In October 2023, the UK introduced a data bridge with the USA in the form of a UK Extension to the EU–USA Data Privacy Framework. The USA data bridge allows the free flow of personal data from the UK to USA-based organisations that are appropriately certified under the scheme without the need for additional transfer mechanism or exception.

For some countries (including the EU), the UK has decided that its data protection regime provides equivalent and adequate safeguards (this is known as an "adequacy decision") and so personal data can be transferred to those countries without additional requirements.

In October 2022, the Department for Digital, Culture, Media & Sport ("DCMS") launched the International Data Transfer Expert Council[5] ("IDTEC"), which was comprised of leading academics and digital industry figures to help the UK capitalise on the opportunities of improved global data sharing.

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 jurisdiction?

In the wider context of international trade, the digitalisation of trade in the UK is intended to improve or enable processes through leveraging digital technologies and digitised data.

This involves the digitalisation of trade-related information flows. Digitalisation will enable the exchange of trade-related data, documents, and electronic authorisations between parties in the supply chain.

Trade digitalisation is attracting greater policy attention as a means to reduce transaction costs, boost trade, lower prices and yield economic growth.

The UK Government has recognised this potential with important policy initiatives under the umbrella of its 2025 Border Strategy. These include the Electronic Trade Documents Act 2023 ("ETDA 2023") (in force from September 2023) and the development of a Single Trade Window, along with commitments negotiated in Free Trade Agreements and Digital Trade

Agreements supporting the development of digital trading systems with trade partners.

The ETDA 2023 is a revolutionary piece of legislation as it provides, for the first time, that certain electronic trade documents, including electronic negotiable instruments, bills of lading and charterparties, to be accorded the same legal status as their paper equivalents if they meet the relevant criteria.

As 80% of global trade transactions choose English and Welsh law as the governing law of contract, the adoption of the ETDA 2023 removed a key barrier to the global expansion of digital trade documents (UK Government, 2022).

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 forward?

A number of domestic and cross-border barriers to implementation are currently in existence. These include computer software interoperability issues and the adoption of model laws into domestic laws. Also, upfront investments and transition costs are seen as key impediments. With regards to blockchain, given that the technology is still in its infancy, a considerable gap exists between the actuality and anticipations.

Moreover, the financial cost of establishing digital trading systems and the time it takes to successfully implement digital trading systems is regarded as a significant barrier.

From a legal and trust perspective, the major barrier to digital contracts concerns legal recognition and security. Many markets still have laws that require physical signatures or stamps on paper documents to be considered legally binding and digital contracts can be more easily challenged in courts. Furthermore, there are anxieties about unauthorised access or the accidental deletion of digital contracts, especially when they are stored in the cloud.

Technical barriers may also involve specific hardware or encryption methods not available in all territories.

Electronic IDs are inevitably limited by national jurisdictions, which may give rise to limited possibilities of cross-border interoperability.

8 Tax Treatment for Digital Businesses

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

Research and Development ("R&D") tax relief supports companies that work on innovative projects in science and technology. To qualify for R&D relief, a project must seek an advance in a field of science or technology.

Only companies chargeable to UK Corporation Tax can qualify for this relief.

The applicable rate for SME R&D tax relief allows companies to deduct an extra 86% of their qualifying costs from their yearly profit, as well as the normal 100% deduction, to make a total 186% deduction.

Alternatively, companies can claim a tax credit if they are loss making, worth up to 10% of the surrenderable loss.

Larger companies can claim an expenditure credit of 20% of their eligible R&D costs.

A business can claim R&D relief up to two years after the end of the accounting period it relates to. It will greatly assist if a summary report that explains how the project meets the gateway definition of R&D, including the technical advances made and the technical uncertainties involved, is submitted with the claim to HMRC.

In addition, Innovation Grants are available for innovative firms to secure funding: business founders do not lose any equity; and the company will never be required to repay the money. Such Government incentives for innovation can help businesses save money on the start-up costs of projects. The amount of funding will be determined by the project's stage, and when awarded earlier in the process, these grants can cover 50% or more of expenditures.

The Enterprise Investment Scheme ("EIS") is a UK Government initiative designed to stimulate investment in early-stage businesses through venture capital; there are four variants available. It serves as a significant source of capital for these companies while also providing attractive tax reliefs to the investors who support them. There is a three-year rule under the EIS that stipulates that investors must hold their EIS shares for at least three years from the date of issue to qualify for the EIS's full tax benefits. This holding period is considered to be of crucial importance, as it ensures that the investment supports the long-term development of the company.

Finally, regarding patents, the Patent Box scheme is designed to encourage companies to keep and commercialise IPR in the UK. It allows companies to apply a lower rate of Corporation Tax to profits earned from its patented inventions. Companies must elect into the Patent Box to apply the lower rate of Corporation Tax, which is 10%.

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?

On a macro level, political leadership is swiftly altering tax and trade policies worldwide. Tax "controversies" predominate across the globe, with governments under pressure to collect revenue.

The importance of Environmental, Social and Governance ("ESG") issues to businesses cannot be underestimated, with investors, lenders, regulators, employees and other stakeholders alike increasingly expecting to understand how ESG fits into a business's strategy. This is likely to see a shift towards greater transparency in tax matters; businesses should be aware of the potential for information reported under these measures to lead to increased tax audits and investigations in the longer term. Digital platform reporting rules are in place to target perceived tax non-compliance by individuals and other persons who provide services or sell goods via online platforms. They operate by requiring the platforms to provide tax authorities with sufficient information to permit those tax authorities to run proper compliance checks on such businesses and individuals. This information is then automatically exchanged with other tax authorities adopting similar rules. In January 2024, the UK introduced similar rules to the EU Directive on Administrative Cooperation in the field of taxation ("DAC7").

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 describe the advantages and disadvantages of the available employment status models.

In the UK, there are three forms of relationship through which employers may employ or engage the services of workers: (i) direct employment; (ii) indirect, casual employment via a third-party agency; and (iii) engagement as a freelance contractor or consultant.

There is a well-established body of statute and case law that has been developed over the decades, aimed at discovering the true status of such a worker under English law. In essence, substance is considered supreme over mere form. Therefore, irrespective of the job description or label that is attached to a worker, the substance of what is actually undertaken is the key consideration. This is a very important task as an employee's rights are greatly superior to those of the self-employed or independent contractor, such as unfair dismissal rights, holiday pay and the National Minimum Wage, as well as discrimination rights. There are also important tax consequences: PAYE with tax deducted at source at each period of pay by employers; or a Schedule D self-assessment of tax, payable in two tranches per year, for the non-employed. The wrong assessment of a worker's status by a fledgling business can result in huge tax liabilities, fines, penalties and interest payments, as well as Employment Tribunal claims, which are free of charge at entry to disgruntled former workers.

The current Government has declared that it is their aim to abolish the practice of zero-hours contracts or the "gig economy", aiming to provide workers with more security and fairness. While a complete ban on zero-hours contracts is not definitively confirmed, the Government is introducing measures to ensure workers have the right to a guaranteed number of hours and compensation for shift cancellations. The Government is using the current Employment Rights Bill (currently at the Committee stage in the House of Lords) as a framework to address these issues.

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

While there is no specific law exclusively for working away from a physical premises, UK working regulations still apply. Workers have a right to request remote and hybrid work from hone ("WFH") and employers may refuse on limited grounds such as that it would have a detrimental effect on quality or performance. There is a tension at the present time between some businesses that do not consider WFH to fit their corporate ethos and workers who consider that it boosts their productivity as they avoid transport time.

Working remotely overseas is a very complex issue, which raises difficult, complex tax and immigration issues.

Employers must adhere to the Health and Safety at Work etc. Act 1974 and the Management of Health and Safety at Work Regulations 1999 to ensure the health, safety, and welfare of their employees, including those working remotely. This includes conducting risk assessments and taking appropriate safety measures.

Employers thus need to ensure that their remote employees are following the laws on working hours, which states that employees should not work more than 48 hours a week.

On 4 October 2023, the ICO published guidance that states that:

> *"Do we need to do a data protection impact assessment (DPIA) before we start monitoring? DPIAs are an important accountability tool. Completing a DPIA helps you to identify and minimise the risks of any monitoring activity you might plan. The DPIA process includes a step where you can discuss your plans to introduce monitoring with workers. This helps to shape your plans and build trust with workers. When carrying out a DPIA you should also consider anyone else captured by your monitoring plans, such as customers, members of the public or household members, if your workers are based at home. You must carry out a DPIA before undertaking any processing likely to cause high risk to workers' and other people's interests. You should use our screening checklists and read our detailed DPIA guidance to help you decide. Examples of high risk processing can include: processing biometric data of workers; keystroke monitoring of workers; monitoring that may result in financial loss (such as performance management); or using profiling or special category data to decide on access to services. If you have a data protection officer (DPO), you must seek and record their independent advice on the outcome of the DPIA before making any final decisions. If, following your DPIA, you decide to go ahead with your proposed monitoring, you must provide information about it to your workers before you begin monitoring. You should carry out a DPIA even if there is no specific high risk as it is a flexible and scalable tool which can assist your decision-making. If you decide to proceed without carrying out a DPIA, you should document your decision. If you have carried out a DPIA which identifies high risk that you cannot reduce, you must consult the ICO before going ahead with the monitoring."*

9.3 What long-term effects or changes are likely to result from the COVID-19 pandemic?

The COVID-19 pandemic has had an indelible impact on the workplace, such that the "post-COVID workplace" is, and will likely continue to be, very different from the one before.

The mass shift to WFH also increased the uptake of the four-day work week, as a number of companies across the UK have allowed their staff to work four days per week without reducing their wages or benefits.

The lack of commute, reduced fuel consumption, and lowered carbon emissions are seen as advantages in many quarters.

It seems that most employers and employees acknowledge that flexible WFH is here to stay into the foreseeable future. It is likely that employers will be flexible and adopt and adjust bespoke WFH modes that best suit their own style of governance and business needs, as well as their employee's specific needs: flexibility being the key concept.

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?

Key legal barriers for digital businesses in the UK include data protection and privacy compliance, intellectual property protection, consumer protection, and adhering to advertising and marketing regulations; in particular, as set out in sections 1, 2 and 3, above.

Additionally, contractual obligations, employment law compliance, and taxation issues can present significant challenges.

The UK GDPR and the DPA 2018 govern how personal data is collected, stored, and used.

Digital businesses must ensure they have vigorous data privacy policies and comply with all relevant regulations, including obtaining consent for data processing, ensuring data accuracy, and implementing appropriate security measures.

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

The Government has stated that "UK Plc" is open for business and that it wishes to encourage and reward entrepreneurship, especially in the AI and e-commerce sphere. It proposes to change the planning regime to make it easier to build digital infrastructure. The Government has also expressed its goal to make the UK a science and technology superpower by 2030.

In addition, there are favourable tax breaks and advantages available to new such businesses as well as favourable grants and funding arrangements.

There is an enhanced emphasis on AI with much work being undertaken in Cambridge and certain locations becoming renown as AI hubs, such as the Warwickshire town of Royal Leamington Spa with its various gaming sector businesses, which have proliferated over the last decade or so.

The Government recently enacted the Digital Assets Act 2024, by which cryptocurrencies are deemed to be capable of passing as property, with the intention of resolving the former confusion as to its status, thereby paving the way for future transactions using crypto.

10.3 What are the key areas of focus of the regulator in your territory for those operating digital business in your territory?

The ICO, as the data protection regulator, is heavily involved in matters affecting all digital business. Areas of focus include: (i) a project to improve cookie compliance; (ii) a consultation on "consent or pay approach" to website cookies (giving users the choice to opt out of cookies for a fee); and (iii) protecting children whilst online, by various steps.

Technology firms with strategic market status will be governed by the Digital Markets, Competition and Consumers Act 2024.

Fintech businesses will need to comply with financial regulations where they offer traditional financial services such as banking, consumer credit and insurance. In addition, the FCA's Regulatory Perimeter (as found in its Guidebook) has evolved to capture innovative fintech markets such as crowdfunding and "buy now, pay later" products and the financial promotion of most cryptoassets, as well as stablecoins.

11 Online Payments

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

In the UK, the online payment sector is primarily regulated by:

i. the Payment Services Regulations 2017 ("PSRs"); and

ii. the Electronic Money Regulations 2011 ("EMRs"),

which implement the EU's Payment Service Directive 2 ("PSD2") and the second Electronic Money Directive ("2EMD").

The UK Government proposed to repeal and replace such legislation, but any such steps seem to be on hold at the present time.

These regulations are overseen by the FCA.

AML and restricting cybercrime are hugely important features of e-commerce in the UK, as they are such pernicious crimes.

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

Regulations around e-commerce generally fall into two areas: (i) distance selling; and (ii) data protection. If an e-commerce business sells products through its own website and/or social media channels, or through online marketplaces, there are rules to be obeyed in order to stay compliant.

When selling products online, certain information must be provided to customers before and after each sale. This consists of providing accurate information on the cost and delivery of the products to ensuring customers can correct errors on their order at any time during the process.

The UK GDPR sets out how a business should collect, store and process its customers' data. By law, a seller must display its data protection policy clearly on its website. The regulation has been put in place to help protect the rights of consumers, and it covers:

- the right to be informed;
- the right of access;
- the right of rectification;
- the right of erasure;
- the right to object;
- the right to data portability; and
- the right to restrict processing.

There are also a number of rights around automated decision-making and profiling.

All these rights have an impact on how a seller displays its information on its digital channels, and how it communicates with its customers.

12 Digital and the Green Economy

12.1 With the current global emphasis on the environment and sustainability, will current or anticipated legislation in that area affect digital business in your jurisdiction?

Yes. Current and anticipated legislation in the UK related to environmental sustainability will significantly impact digital businesses. This is because the digital sector has a substantial environmental footprint, and regulations aim to reduce this impact through various means.

The UK's focus on net-zero emissions, coupled with new laws like the Environment Act 2021, and the push for sustainable practices in digital procurement and operations will compel changes in how digital businesses operate.

12.2 Are there any incentives for digital businesses to become 'greener'?

Almost £5 billion of UK Government funding is available to help UK businesses become greener as part of the Government's commitment to reach net-zero emissions by 2050.

To make it easier for small businesses to find funding, the Government recently launched their Find a Grant service. This can be used to search for funding across the country, which can help a business to increase energy efficiency and decrease carbon emissions.

There are several green financing options available from major banks across the UK.

The SME Loan Scheme in Scotland supports businesses with the installation of energy efficient systems, including heat pumps, biomass boilers and air conditioning upgrades. Through this scheme, business owners can receive a loan of up to £100,000 and a cashback grant of up to £30,000.

The Small Business Bonus Scheme in Scotland provides business premises owners with rates relief. The rates relief varies depending on the rateable value of the premises. To be eligible for this scheme, the business premises must have a rateable value of £20,000 or less.

12.3 What do you see as the environmental and sustainability challenges facing digital businesses?

Digital businesses in the UK face significant environmental challenges related to energy consumption, e-waste, and the embodied emissions of hardware and infrastructure.

Data centres, user devices, and network infrastructure contribute to carbon emissions, and the rapid growth of digital technologies exacerbates these impacts. Additionally, the disposal of electronic waste and the extraction of resources for manufacturing pose environmental threats.

The development and training of AI models require significant computational power and energy, which can contribute to higher emissions. The growing amount of data being stored in the cloud requires energy-intensive data centres.

While WFH can reduce commuting-related emissions, it can also increase energy consumption for devices and infrastructure at home.

The lack of comprehensive data and divergent methodologies make it difficult to accurately calculate the carbon emissions of digital technologies.

The absence of common standards for measuring and reporting sustainability metrics hinders progress.

Endnotes

1 https://www.statista.com/forecasts/891311/digital-buyer-penetration-in-the-united-kingdom

2 https://www.statista.com/forecasts/891317/digital-buyer-penetration-in-europe

3 https://newsroom.accenture.com/news/2023/one-billion-new-online-shoppers-are-entering-the-market-creating-significant-growth-opportunities-for-digital-commerce-finds-new-study-by-accenture

4 https://www.drcf.org.uk/projects/projects/international-network-for-digital-regulation-cooperation-indrc

5 https://www.gov.uk/government/news/global-data-experts-fire-up-governments-plans-to-promote-free-flow-of-data

Andrew Maguire is an experienced chancery commercial barrister, who has specialised in banking and financial services for over 25 years, such as succeeding in the all-monies guarantee Court of Appeal case of *NMBS v Bellamy* [2013] EWCA Civ 452. More recently, his practice has increasingly involved data protection and international crypto and blockchain fraud. He successfully obtained the first summary judgment against a crypto exchange, using a constructive trust between an exchange and investor, which was served by NFT airdrop: see *Jones v Persons Unknown/Huobi* [2022] EWHC 2543; and the reported case in *WLR of Mooij v Persons Unknown* [2024] EWHC 2342 (Ch); [2025] 1 WLR 821.

Andrew is regularly instructed in financial services investment scam cases requiring urgent relief, mostly with an overseas dimension involving cross-border claims. In addition, Andrew regularly advises and acts for firms and individuals regarding the FCA's Guidebook fintech obligations and requirements, many with an overseas element to the claim.

Andrew is ranked in *The Legal 500* as a leading senior counsel at the London Bar in four categories: Crypto and Blockchain Assets (Tier 1); Financial Services and Fintech Regulation (Tier 2); Commercial Disputes; and Banking and Finance.

Littleton Chambers
3 King's Bench Walk, Temple
London EC4Y 7HR
United Kingdom

Tel: +44 20 7797 8600
Email: amaguire@littletonchambers.co.uk
LinkedIn: www.linkedin.com/in/andrew-maguire-99a29a16

Littleton Chambers is a highly respected and long-established set of barristers' chambers, located in the heart of the legal district at the Temple, London. Renowned for its excellence in both employment and commercial law, Littleton is consistently recognised as a leading set, offering top-tier advocacy and advisory services to clients across a broad spectrum of practice areas. The Chambers is frequently instructed by top-ranked national and international law firms to act in some of the most high-profile and complex legal matters in the UK and internationally.

Littleton has a dynamic team of 54 members, including 17 KCs and highly regarded juniors. Littleton members' practices cover a wide spectrum of work, including employment law, business protection, and commercial law incorporating civil fraud, as well as insolvency, financial services, banking, commercial contracts, share and business sale agreements, and shareholder disputes. Their expertise also covers company and partnership law, disciplinary and regulatory injunctions, arbitration, mediation, investigations, sport, and international and offshore disputes.

Littleton is set apart by its strong emphasis on commercial awareness, client-focused service, and practical, strategic advice. Members of Chambers are known for combining intellectual rigour with a down-to-earth approach and are user-friendly.

Recent quotes from *The Legal 500 2025* include: *"Littleton Chambers is well-regarded for its depth of expertise in commercial law. They have a broad range of experienced barristers available and offer strong training programmes that ensure high standards across the board"*; and *"[t]heir reputation for excellence in service delivery has made Littleton a go-to choice for solicitors, in-house counsel and clients facing complex disputes"*.

www.littletonchambers.com

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Digital Business 2026 features one expert analysis chapter and 18 Q&A jurisdiction chapters covering key issues, including:

- E-Commerce Regulation
- Data Protection
- Cybersecurity Frameworks
- Cultural Norms
- Brand Enforcement Online
- Data Centres and Cloud Location
- Trade and Customs
- Tax Treatment for Digital Businesses
- Employment Law Implications for an Agile Workforce
- Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions
- Online Payments
- Digital and the Green Economy

The International Comparative Legal Guides are published by: glg Global Legal Group