PANORAMIC

DIGITAL BUSINESS

Cyprus

LEXOLOGY

Digital Business

Contributing Editor

Ashley Winton

Mishcon de Reya LLP

Generated on: March 11, 2024

Contents

Digital Business

UPDATE AND TRENDS

Key trends and developments

Contributors

Cyprus

Antoniou McCollum & Co LLC

Anastasios A Antoniou anastasios.antoniou@amc.law
Ifigenia Iacovou ifigenia.iacovou@amc.law
Orestis Anastasiades orestis.anastasiades@amc.law

LEGAL AND REGULATORY FRAMEWORK

Government approach

How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

Recent years have seen substantive policy initiatives aimed at digital transformation. At the core of recent policy initiatives is the creation of the Deputy Ministry of Innovation, Research and Digital Policy. The Deputy Ministry developed the digital strategy for Cyprus up to 2025, which is currently being implemented. Updated regulatory frameworks are now in place to govern online business and transactions.

Law stated - 28 September 2023

Legislation

What legislation governs digital content and services, digital transformation and the conduct of business online?

A wide range of statutes and regulations governs the following domains:

- the provision of digital content and digital services into Cyprus;
- electronic commerce and aspects of electronic commercial contracts;
- the conclusion of online consumer contracts;
- the protection of consumers when purchasing products and services online;
- the conclusion of contracts of the sale of products online;
- the provision of electronic communications services into Cyprus;
- the security of network and information systems (cybersecurity); and
- personal data protection.

Law stated - 28 September 2023

Regulatory bodies

Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, artificial intelligence, internet access and telecommunications?

The Ministry of Energy, Commerce and Industry is competent for the supervision and effective enforcement of the regulatory framework concerning electronic commerce.

The competent authority for the enforcement of the personal data protection framework in Cyprus is the Commissioner for the Protection of Personal Data (the DPC). The DPC assesses potential infringements of Regulation (EU) 2016/679 on the protection of natural persons with regard t

o the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)) and Cypriot data protection laws, whether on its own initiative or following a complaint, and can impose sanctions on finding an infringement.

The Communications Commissioner (the CC) is the competent authority in Cyprus for the regulation of Internet access in Cyprus. The CC is competent to safeguard an open Internet and ensure consumers of electronic communication services in Cyprus are protected.

The CC also has the power to determine applicable charges and tariffs, including the minimum and maximum tariff thresholds to ensure fair competition, transparency and cost-effectiveness between electronic communications. On finding an infringement of the applicable framework, the CC can impose administrative fines or other sanctions.

The Department of Electronic Communications is a department in the Deputy Ministry of Research, Innovation and Digital Policy, and oversees the national broadband plan of Cyprus.

The Digital Security Authority (the DSA) is competent for the implementation and enforcement of the applicable framework concerning network and information systems security. The DSA is tasked with receiving reports of any cybersecurity incidents by service providers and operators to which the relevant framework applies and to ensure that service providers and operators take appropriate measures to prevent and minimise the impact of incidents affecting the security of networks and information systems. The DSA also supervises the national CSIRT (CSIRT-CY) and ensures that it has access to appropriate, secure and robust communications and information infrastructure at national level, and ensures cross-border cooperation with competent authorities in other jurisdictions.

Law stated - 28 September 2023

Jurisdiction

What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

EU rules apply to disputes involving defendants selling goods or services from an EU member state to Cyprus. Subject to exceptions, the default position is that defendants domiciled in an EU member state shall, regardless of their nationality, be sued in the courts of that member state. Cypriot courts have consistently applied the EU rules on jurisdiction, including with respect to online transactions.

The rules of jurisdiction may, under certain circumstances, apply to parties domiciled outside the EU, such as the parties to a contract agree that the courts of an EU member state should have jurisdiction. Online traders often use standard terms and conditions and a jurisdiction clause in such standard terms and conditions may satisfy the requirement to confer jurisdiction of the courts of a particular EU member state.

Restrictions apply with respect to sales of goods or services or the provision of digital content to a consumer in Cyprus. A consumer is able to bring proceedings in the courts of Cyprus, rather than those where the digital business is domiciled.

The above rules have not yet been tested in respect of transactions in the metaverse by Cyprus courts.

Law stated - 28 September 2023

Establishing a business

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

Establishing a business in Cyprus to provide services online may require authorisation from competent authorities in certain industries. Such industries include payment services, financial services, banking services, insurance services and electronic communications.

With respect to digital content, establishing a media service provider or a video-sharing platform provider is subject to relevant regulatory authorisations.

Law stated - 28 September 2023

CONTRACTING ON THE INTERNET

Contract formation

Is it possible to form and conclude legal contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

Yes, contracts can be concluded digitally, between businesses (B2B), between businesses and consumers (B2C) and in a non-commercial context. Cyprus law recognises the digital conclusion of contracts.

The consumer protection framework applies to consumer contracts, in which cases mandatory information, language and other formalities must be adhered to by the trader, both at a pre-contractual stage and in the trader's terms of sale.

Law stated - 28 September 2023

Applicable laws

Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

The seller of goods or services online must provide the purchaser, whether a business or a consumer, with some key information. Such information includes the governing law of the contract and the languages offered for the conclusion of the contract.

With respect to consumers in particular, online traders must provide certain information in Greek (or in the language of choice of the consumer where the trader agrees to such choice of language). Such information includes, where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

While the terms of a contract can specify laws other than the laws of Cyprus to govern an online contract, a consumer cannot be deprived of the protection afforded under Cyprus consumer protection legislation where the foreign governing law offers a lower level of protection.

Law stated - 28 September 2023

Electronic signatures

How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction? What type of digital information can be signed and how does the signing take place?

Electronic signatures in Cyprus are regulated by the applicable EU framework and national implementing legislation. The Department of Electronic Communications of the Ministry of Transport, Communications and Works of the Republic of Cyprus (the DEC) is the competent authority for the implementation and enforcement of the applicable framework on electronic signatures in Cyprus.

The types of electronic signatures recognised under Cyprus law are the following:

- An electronic signature, which is defined as data in electronic form that is attached to or logically associated with other data in electronic form and that is used by the signatory to sign.
- An advanced electronic signature, which is defined as an electronic signature that meets the following requirements: it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control; and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
- A qualified electronic signature, which is defined as an advanced electronic signature that is created by a qualified electronic signature creation device and that is based on a qualified certificate for electronic signatures.

A qualified certificate for electronic signatures for the purposes of the qualified electronic signature, is issued by a qualified trust service provider. A qualified electronic signature will have the equivalent legal effect of a handwritten signature.

Law stated - 28 September 2023

Breach

Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

There are no special forums for a case of breach of a digital contract. Subject to jurisdictional rules, Cypriot courts can hear claims alleging breaches of digital contracts.

In relation to consumer contracts, consumers can use the Online Dispute Resolution platform provided by the European Commission for the online resolution of disputes between consumers and businesses. Submission of complaints is usually carried out though the national contact points.

Law stated - 28 September 2023

FINANCIAL SERVICES

Regulation
Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

In the absence of passporting of an investment firm's licence from another EU member state into Cyprus, advertising or selling financial services products in Cyprus may be subject to authorisation by the Cyprus Securities and Exchange Commission (CySEC). CySEC may impose administrative sanctions for breach of licensing or passporting requirements and criminal liability may also become relevant in cases of unauthorised financial services activities in Cyprus.

Where banking or payment services are provided in breach of the respective licensing or passporting requirements in Cyprus, the providers involved may be subject to administrative sanctions that can be imposed by the Central Bank of Cyprus.

Marketing communications addressed by an investment firm to clients or potential clients must be clearly identifiable as such and be fair, clear and not misleading. Certain key requirements applicable to direct marketing of financial services are the following:

- an opt-in requirement applies to unsolicited communications;
- using electronic contact details already provided by the client to directly market a provider's similar products or services should take place only where the client is clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and with every future instance of marketing communication; and
- direct marketing emails are prohibited if they disguise or conceal the identity of the sender and do not include a valid address to which the recipient may send a request for ceasing such communications, or that encourages recipients to visit websites.

Under Cypriot consumer protection legislation, misleading and aggressive commercial practices carried out by any consumer-facing business would constitute unfair commercial practices, which are prohibited under the Consumer Protection Law. These rules will also apply to the advertising of financial services via the internet.

Law stated - 28 September 2023

Electronic money and digital assets

Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

The Central Bank of Cyprus is the competent authority for the authorisation and supervision of electronic money services providers in Cyprus. Issuing electronic money is an activity that can only be carried out in Cyprus inter alia by authorised credit institutions and electronic money institutions. Electronic money services may also be offered from within Cyprus by electronic money institutions authorised under the laws of another EU member state, under the right of establishment and the freedom to provide services.

Law stated - 28 September 2023

Digital and crypto wallets

Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

Providers of crypto wallets may be subject to authorisation by CySEC, depending on their precise activities. Activities that require CySEC's authorisation include the following:

- reception and transmission of client orders in crypto-assets;
- execution of orders on behalf of clients in crypto-assets;
- exchange between crypto-assets and fiat currency or between crypto-assets;
- participation in or provision of financial services related to the distribution, offering or sale of crypto-assets, including the initial offering;
- placement of crypto-assets without firm commitment;
- crypto-asset portfolio management;
- administration, transfer of ownership, transfer of site, holding, or safekeeping, including custody, of crypto-assets or cryptographic keys or means enabling control over crypto-assets;
- underwriting or placement of crypto-assets with firm commitment; and
- operation of a multilateral system, which brings together multiple third-party buying and selling interests in crypto-assets in a way that results in a transaction.

Law stated - 28 September 2023

Electronic payment systems

How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

Payment institutions can engage in carrying out the operation of payment systems. The Central Bank of Cyprus (the CBC) is the competent authority for the authorisation and supervision of payment services providers in Cyprus, including payment systems.

Under the provisions of the law, payment systems cannot impose on, inter alia, payment service users (ie, payers of payees) any of the following requirements on access:

- restrictive rules for effective participation in other payment systems;
- any rules discriminating between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; or
- any restrictions on the basis of institutional status.

Payment systems are only permitted to process personal data when it is necessary to safeguard the prevention, investigation, detection and prosecution of payment fraud. Any processing must be carried out in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). Any access, processing and retention of users' personal data necessary for the provision of the payment services, can only take place with the consent of end customers (ie, payment service users).

Law stated - 28 September 2023

Online identity

Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

The Central Bank of Cyprus (CBC) is the competent authority for AML and KYC requirements in respect of providers of banking services, payment services and electronic money institutions. The Cyprus Securities and Exchange Commission (CySEC) is respectively tasked with supervising providers' investment services with respect to the AML and KYC requirements that they apply to their business relationships and transactions.

The CBC and CySEC issue subsidiary legislation to regulate AML and KYC requirements pursuant to the provisions of national AML legislation. Cyprus law has transposed the EU AML directives (including Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing).

Reliance on third parties for the implementation of procedures for customer identification and due diligence measures must be done where the third parties are themselves regulated and supervised in accordance with the requirements of applicable law. Nevertheless, the

service provider remains liable for compliance with the applicable law at all times, and such liability is not subject to delegation to any third party.

Law stated - 28 September 2023

DOMAIN NAMES AND URLS

Registration procedures

What procedures are in place to regulate the registration of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident or business in the country? Are there any restrictions around the use of URLs to direct users to particular websites, online resources or metaverses?

The country code top-level domain (TLD) name for Cyprus is '.cy'. The competent regulatory authority is the Communications Commissioner (CC). The University of Cyprus (UCY) was appointed by the CC to regulate to handle the .cy TLD, including licensing.

The .cy TLD is divided into several secondary level (Level-B) domain names, each of which describes a specific service. Depending on the type of activities, a company or organisation may opt to be registered with a secondary domain name.

Applicants from any country can apply for a .cy domain name.

Law stated - 28 September 2023

IP ownership

Can domain names or URLs be the subject of trademark or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

The right to use a .cy domain under a licence granted by the UCY does not confer copyright or trademark-related rights. In considering an application for the registration of a domain name, the UCY does not investigate whether the applicant is the right holder of any rights on the name included in the domain name or is otherwise authorised to use such name. The domain name applicant is responsible to ensure that the name applied for does not infringe the intellectual property of any other party.

The registration of a domain name may be subject to challenge by a third party claiming rights over the domain name due to ownership of a trademark. A third party may apply to the UCY for the revocation of any decision of the UCY to assign a right to use or register a domain name, proving ownership of the trademark.

Law stated - 28 September 2023

ADVERTISING

Regulation

What rules govern online advertising?

An online advertisement to Cypriot users must:

- be clearly identifiable as a commercial communication; and
- clearly identify the person on whose behalf the commercial communication is sent.

If the communication is unsolicited, it must be clearly and unambiguously identifiable as such, as soon it is received.

Rules concerning misleading and aggressive advertising also apply to online advertising to consumers in Cyprus.

Law stated - 28 September 2023

Targeted advertising and online behavioural advertising

What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The framework on targeted advertising and online behavioural advertising in Cyprus applies to cookies, bots and any technology that collects, has access to, shares, processes or monitors one or more identifiers or technical equipment of a subscriber or user.

Automated individual decision-making, including profiling is governed by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). Under the GDPR, a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them unless such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or unless such decision is based on the data subject's explicit consent. However, the controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. In any event, the data subject must have the right to object at any time, to the processing of personal data for profiling purposes.

Information on cookies must be 'clear and comprehensive'. The user must clearly provide their consent to the use of cookies by a website. Mere information that a website uses cookies and that users automatically accept cookies by browsing the website, does not meet the statutory requirements. Consent must be given in the form of an affirmative action. In particular, the Commissioner for the Protection of Personal Data (the DPC) highlights in the DPC Guidance that consent cannot be implied from use of the website and indicates that it must be clear that a user has actively engaged with a cookie banner to unambiguously consent to use of cookies.

Where cookie banners are used, they must not indirectly force a user to accept all cookie; both accept and reject options should be clearly provided on the banner. Also, due to the voluntary nature of consent, where the user is not able to access the service or website in the absence of express consent to cookies, this would mean that the website does not present

the user with a genuine choice, therefore it cannot be deemed valid consent as it is not freely given.

Nevertheless, the requirement of the user's consent for the use of cookies is not required:

- for technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network ('communications exemption'); or
- as strictly necessary to provide an information society service explicitly requested by the subscriber or user ('strictly necessary exemption').

The validity period of consent would depend on various factors, including whether the purposes of processing have changed and the period for which the personal data will be stored that the controller shall be determined and communicated to the user.

While the framework does not provide for a specific retention period for cookies, if the collected data constitutes personal data, the provisions of the GDPR must be complied with and such data must not be kept for longer than necessary for the purposes for which the personal data are processed.

'Dark patterns' are also relevant to targeted advertising and online behavioural advertising. Dark patterns, defined by the European Data Protection Board as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. The data protection principles applicable to dark patterns are those set out in article 5 the GDPR.

Law stated - 28 September 2023

Misleading advertising

Are there rules against misleading online advertising?

Misleading and aggressive commercial practices carried out online by any consumer-facing business would constitute unfair commercial practices, which are prohibited.

Advertisers should make sure that any advertisement as well as its overall presentation and any statements used for commercial reasons do not include any false information and all statements used in the commercial communication are true and verified. The advertisement should also not omit any essential information that the consumer would need, to make an informed decision on the transaction.

Advertisers should keep a record where possible of proof of any market surveys carried out to determine the average consumers views and expectations as to the specific product advertised. Furthermore, any reference to the product's price should be supported by records of price calculations leading to the advertised price. Generally, any competitive claim must be substantiated with relevant evidence. These rules apply to all advertising directed towards consumers. At the same time, specific rules apply to certain industries – for example, electronic communications.

Law stated - 28 September 2023

Restrictions

Are there any digital products or services that may not be advertised online?

Audiovisual commercial communications displayed online by media service providers and video-sharing platform providers that fall under the jurisdiction of Cyprus are subject to a wide range of restrictions, whether they concern digital or other products. Several restrictions apply for the protection of minors, such as the prohibition of advertising that may harm minors. Additional restrictions are applicable to prevent any advertising that includes or promotes discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation, encourages behaviour prejudicial to health or safety, encourages behaviour grossly prejudicial to the protection of the environment.

Regarding specific products, it is prohibited to advertise cigarettes and other tobacco products, electronic cigarettes and medicinal products and medical treatments available in Cyprus on prescription. Alcoholic beverages advertisements must not be aimed specifically at minors and shall not encourage immoderate consumption of such beverages.

Law stated - 28 September 2023

Direct email marketing

What regulations and guidance apply to email, SMS and other direct marketing?

The following apply with respect to unsolicited marketing communications, including emails:

- prior consent of the recipient for direct marketing communications is required (including via email, SMS and automated calling); and
- using electronic contact details already on file to directly market a provider's similar products or services may take place only where the recipient is clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their details at the time of their collection and with every future instance of marketing communication.

Marketing communications addressed to consumers must have the consumer's prior consent as to the means of communication. Direct marketing emails that disguise or conceal the identity of the sender, and which do not include a valid address to which the recipient may send a request for ceasing such communications, are not allowed.

Where personal data is processed for direct marketing purposes, the data subject will have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Under article 21 of the GDPR, where the data subject objects to processing for direct marketing purposes, any further processing of the data subject's personal data for such purposes would constitute a breach of the provisions of the GDPR.

In the context of banking, credit, insurance, investment or payment services, the consumer's prior consent is required before a service provider performs distance communication techniques using automated calling systems without human intervention.

Law stated - 28 September 2023

ONLINE PUBLISHING

Hosting liability

What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Where a content provider or a party that is merely hosting content has no actual knowledge of illegal content and is not aware of facts or circumstances from which such activity is apparent, the safe harbour defence is available and the content provider or hosting party may be exempt from liability. Under Cyprus law internet service providers (ISPs) are exempt from liability for content that is hosted on their sites. Liability may occur in the event the host has actual knowledge or awareness of facts or circumstances in which illegal content is apparent. Once such knowledge or awareness is obtained; the host provider must meet takedown or shutdown obligations.

The safe harbour defence may not be strong when invoked in respect of content over which the ISP has editorial control. A case-by-case assessment of the precise facts and circumstances is necessary to determine whether the safe harbour defence can successfully be invoked by any party.

Law stated - 28 September 2023

Content liability

When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

A digital platform or online content provider may be liable under Cyprus law for mistakes in information that it publishes online where this information would cause a consumer to make a purchasing decision that they would not have taken otherwise. Such mistakes in information may also lead to liability where they are found to amount to misleading advertising – that is, where these are found to affect the economic behaviour of consumers or to be detrimental to a competitor. Liability for such mistakes in information may occur by virtue of the failure to meet information requirements that are imposed by the relevant legislative framework on consumer protection and electronic commerce.

Liability may be mitigated through the use of notices to delimit the reasonable expectations of the recipient of the information. However, liability cannot be excluded where information is clearly and unambiguously misleading.

Law stated - 28 September 2023

Shutdown and takedown

Can an internet service provider or telecommunications provider shut down a web page containing defamatory material provided by a third party without court authorisation?

Online content providers or ISPs may shut down web pages containing defamatory material without court authorisation.

Law stated - 28 September 2023

INTELLECTUAL PROPERTY

Data and databases

Are data and databases protected by IP rights?

Data and databases enjoy general copyright protection under the law. Databases, in particular, enjoy such general copyright protection where the selection or arrangement of their contents constitutes the creator's own intellectual creation. Moreover, the database is subject to a specific, sui generis type of intellectual property right allowing the creator of such database to prohibit the unauthorised extraction or reuse of its contents.

Law stated - 28 September 2023

Third-party links and content

Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Linking to third-party websites or platforms without permission may, under certain circumstances, constitute an infringement of intellectual property rights. The established legal precedent on this matter suggests a case-by-case, individualised approach in determining whether linking constitutes an infringement. Relevant considerations that are assessed include:

- whether the communication is for profit;
- whether the right holder of the intellectual property has initially provided consent for the linked content and the level of care undertaken to confirm this;
- whether the link to the content allows users to circumvent restrictions that make the content accessible to subscribers only; and
- whether the illegal nature of the content has been notified by the right holder.

Law stated - 28 September 2023

Third-party links and content

Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

Under current Cyprus law, using third-party content that is obtained via automated scraping or otherwise, without permission from the third-party content provider, may constitute an infringement of copyright or other intellectual property rights.

Law stated - 28 September 2023

Metaverse and online platforms

Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

Copyright and database protection would arise for both the computer programs through which a metaverse is operated and for works created in such metaverse. When the metaverse allows users to create works (ie, it is an 'open' metaverse), such works would be protected by copyright. Difficulties are expected when pursuing infringement proceedings with respect to copyright or database rights on a metaverse, as the identity of the infringer may be difficult to ascertain.

As trademarks present a strong territoriality element with respect to their protection, enforcement actions may face difficulties in establishing a potential infringement of a trademark on a metaverse, to the extent it cannot be ascertained which jurisdiction's trademark protection rules would apply.

Law stated - 28 September 2023

Exhaustion of rights and first-sale doctrine

Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

Exhaustion of rights is recognised in Cyprus. The distribution right in the EU is only exhausted if the first sale or other transfer of ownership in the EU is made by the copyright owner or with their consent. The exhaustion of rights does not generally apply to downloadable digital content for permanent use and right holders may be able to restrict resales of such digital content.

Law stated - 28 September 2023

Administrative enforcement

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

Police authorities may carry out searches in private premises under a search warrant when investigating IP infringements that may involve a criminal offence. Freezing injunctions are generally available by Cypriot courts with respect to IP infringement, when the relevant conditions are met.

Law stated - 28 September 2023

Civil remedies

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

IP owners can pursue remedies for infringement of their IP rights, including damages. When applicable requirements are met, IP owners may be able to apply to court for search orders or freezing injunctions, as well as orders for the destruction or delivery of the copies that infringe copyright, the tools used and an order for account of profits achieved as a result of the infringement.

Law stated - 28 September 2023

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The personal data protection framework in Cyprus comprises:

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)); and
- the Protection of Natural Persons against Processing of Personal Data and t he Free Movement of such Data Law of 2018(L.125(I)/2018) as amended (the Law).

The competent authority responsible for the enforcement of the GDPR and the Law in Cyprus is the Commissioner for the Protection of Personal Data (the DPC).

The definition of 'personal data' under the Law reflects the definition of personal data under article 4 the GDPR.

Special categories of personal data are protected in Cyprus under the provisions of article 9 of the GDPR. Such categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Under the GDPR there is an express prohibition on the processing of special categories of personal data, save for specific exceptions, including where the data subject has given their explicit consent to such processing for specific purposes. The Law prohibits the processing

of genetic and biometric data for the purposes of health and life insurance. Also, where processing of such personal data is based on explicit consent, any further processing requires a separate consent.

Personal data provided on an anonymised basis would generally not constitute personal data for GDPR purposes. Pseudonymisation would, under specific circumstances, be deemed an alternative to anonymisation where it has the effect of removing 'personal data'. Where pseudonymised data still lead to an identifiable individual under the circumstances, pseudonymisation would not have the effect of anonymisation.

Law stated - 28 September 2023

Registration and appointment of data protection officer

Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

No registration is required prior to the processing of personal data under Cyprus law.

Article 37 of the GDPR specifically requires the designation of a data protection officer where:

- processing of personal data is carried out by a public authority or body (irrespective of what data is being processed);
- the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Law stated - 28 September 2023

Extraterritorial issues

Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The GDPR applies to:

- controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place within the EU; and
- non-EU controllers and processors with no EU establishment that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU.

Business that are not established in the EU but to which the GDPR applies must designate, in writing, a representative in one of the EU member states in which data subjects are affected

by the processing concerned. This requirement will not apply if the controller is a public authority or body. This requirement will also not apply if:

- the processing is occasional or it constitutes large-scale processing of special categories of personal data or criminal convictions and offences; and
- is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing.

Law stated - 28 September 2023

Bases for processing

What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

Processing personal data is lawful when carried out on one of the grounds provided for under article 6 of the GDPR.

Commonly invoked bases for processing personal data include:

- consent given by the data subject to the processing of their personal data for specific purposes;
- where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and
- where processing is necessary for the legitimate interests pursued by the controller.

Any processing of personal data must be in line with the Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data Law of 2018 (L.125(I)/2018) as amended (the Law) and the GDPR. The competent authority responsible for the enforcement of the GDPR and the Law in Cyprus is the Commissioner for the Protection of Personal Data (the DPC).

Under the GDPR there is an express prohibition on the processing of special categories of personal data, save for specific exceptions, including where the data subject has given their explicit consent to such processing for specific purposes. The Law prohibits the processing of genetic and biometric data for the purposes of health and life insurance. Also, where processing of such personal data is based on explicit consent, any further processing requires a separate consent.

No additional restrictions apply with respect to transfers of personal data within the EU. However, as the carrying out of the personal data transfer will in all cases constitute processing of personal data, the GDPR principles relating to lawful processing will still apply.

The transfer of personal data to a country for which an adequacy decision has been issued by the European Commission may be performed without restrictions. If there is no adequacy decision for a third country, for a third-country personal data transfer to be lawful, personal data must be sufficiently protected by way of standard contractual clauses, binding

corporate rules, European Commission-approved codes of conduct, or by way of certification of the data processing procedure.

In the absence of an adequacy decision or appropriate safeguards, article 49 of the GDPR may be invoked to permit a data transfer to a third country on the basis of a derogation. Such derogations would include:

- explicit consent by the data subject after being informed of the data transfer risks due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- the transfer is necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- the transfer is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent;
- the transfer is necessary for important reasons of public interest or to establish, exercise or defend legal claims;
- the transfer is made from a public register that is intended to provide information to the public and specific conditions are fulfilled; and
- the transfer is in the controller's legitimate interests.

A transfer of personal data to a third country based on a derogation requires carrying out an impact assessment and prior consultation with the DPC.

Law stated - 28 September 2023

Data export and data sovereignty

Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules that require data, data servers or databases to remain in your jurisdiction?

Personal data may be transferred to a third-country jurisdiction only in compliance with the applicable provisions of the GDPR.

The transfer of personal data to a country for which an adequacy decision has been issued by the European Commission may be performed without restrictions. If there is no adequacy decision for a third country, for a third-country personal data transfer to be lawful, personal data must be sufficiently protected by way of standard contractual clauses, binding corporate rules, European Commission-approved codes of conduct, or by way of certification of the data processing procedure.

The transfer of special categories of personal data – that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation – to a third country may, under certain circumstances, require prior consultation with the Data Protection Commissioner of Cyprus, which is legally

empowered to impose restrictions on such transfer. In this respect, an impact assessment may also be required.

There are no data sovereignty or national security rules that require data, data servers or databases to remain in Cyprus.

Law stated - 28 September 2023

Sale of data to third parties

May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

Sales of personal data to third parties would involve a transfer of personal data. Transfers of personal data are regulated by the GDPR. Any transfer of personal data by either a controller or a processor to any third party will under any circumstances constitute processing of personal data. No additional restrictions apply to the sale of personal data, provided that the requirements of the GDPR for such processing are complied with.

Law stated - 28 September 2023

Consumer redress

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

Cypriots and non-Cypriots are afforded the same protection under the GDPR and the Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data Law of 2018 (L.125(I)/2018), as amended (the Law), when their personal data is processed in Cyprus.

Key rights under the GDPR are the following:

- Right of access – right to obtain information from the controller as to whether or not his or her personal data are processed, the envisaged period for which the personal data will be stored, the purpose for which they are processed, any recipients and as to his or her rights under the GDPR. The Commissioner for the Protection of Personal Data (the DPC) has clarified that the right of access is provided to individuals free of charge. The DPC also advises the controller to respond to such request for access at least within one month from receipt of such request.
- Right to rectification – right to obtain without undue delay the rectification of inaccurate personal data concerning him or her.
- Right to erasure ('right to be forgotten') – right to obtain the erasure of personal data concerning him or her without undue delay. When an individual exercises this right and the personal data are no longer necessary in relation to the purposes for which they were collected or processed, or there is no longer a legal ground for processing after the data subject withdraws his or her consent, or they have been unlawfully processed or they have to be erased for compliance with a legal obligation of the controller, or

they have been collected in relation an information society services offering, then the controller must erase the data without undue delay.

- Right to restriction of processing where the accuracy of the personal data is contested by the data subject.
- Right to data portability – right to receive the personal data concerning him or her in a machine-readable format and to transmit such data to another controller without hindrance from the controller or to transmit such data directly from one controller to another, where processing is based on consent or on the performance of a contract and the processing is carried out by automated means.
- Right to object, at any time, to processing, on grounds (e) or (f) of article 6(1) of the GDPR, of personal data concerning him or her, including profiling based on those provisions. Following the exercise of this right, the controller can only process the personal data if it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Right to lodge a complaint with the competent authority responsible for the enforcement of the GDPR and the Law in Cyprus – ie, the Commissioner for the Protection of Personal Data.

Law stated - 28 September 2023

Non-personal data

Does the law in your jurisdiction regulate the use of non-personal data?

Non-personal data in Cyprus is regulated at EU level. Main EU level regulation governing the use of non-personal data is Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. There is currently no other specific local law governing non-personal data usage in Cyprus.

Law stated - 28 September 2023

DOCUMENT DIGITISATION AND RETENTION

Digitisation

Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

Under the laws of Cyprus, digital representations of documents or record types are afforded the same evidentiary value as their original paper form counterparts. As such, there is no requirement to keep any particular document or record types in original paper form.

Law stated - 28 September 2023

Retention

Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

Documents or other record types that are collected for the purposes of compliance with anti-money laundering legislation must be retained for at least five years after the end of a business relationship with the customer or the conclusion of a one-off transaction. For tax compliance purposes, documentation and other records relevant to the calculation and imposition of taxation in Cyprus should be kept for up to seven years. Furthermore, considering the statutory limitation periods for bringing a civil claim under Cyprus law, which periods vary depending on the nature of the claim, it is advisable that documents or other record types that may be linked to a potential claim are kept for up to 10 years.

Law stated - 28 September 2023

DATA BREACH AND CYBERSECURITY

Security measures

What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

Cyprus law provides for precautionary measures that should be taken by providers of publicly available electronic communications services to avoid data breaches and ensure cybersecurity. Such minimum precautionary measures require that providers must:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and
- ensure the implementation of a security policy with respect to the processing of personal data.

Essential services providers and critical infrastructure providers must implement measures relating to the annual risk assessment of their network information systems, their business continuity plans and disaster recovery plans, their compliance with standards adopted at EU level and ensure the business integrity of their networks.

Law stated - 28 September 2023

Data breach notification

Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Data breaches and relevant notification requirements are regulated under article 33 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). The GDPR is supplementary to the Cyprus Law on Protection of Natural Persons against Processing of Personal Data and the Free Movement of such Data of 2018 (L.125(I)/2018) as amended (the Law). The national competent authority responsible for the enforcement of the GDPR and the Law in Cyprus, which accepts data breach notifications, is the Commissioner for the Protection of Personal Data (the DPC).

A controller must notify a personal data breach to the DPC without undue delay and, where feasible, not later than 72 hours after having become aware of it, or provide reasons for the delay. Furthermore, when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the data breach to the data subject without undue delay in accordance with the provisions of article 34 of the GDPR.

Personal data breaches that result from cybersecurity breach incidents are also governed under national legislation that transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union into Cyprus law. Under this legislation, essential services providers, digital service providers, providers of electronic communication services and networks must take appropriate security measures and notify serious incidents to the Digital Security Authority.

Law stated - 28 September 2023

Government interception

Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

Law enforcement authorities can access data for the purposes of investigating the perpetration of criminal offences. Such authorities include the Police, the Customs and Excise Department, the Tax Department and the Anti-Money Laundering Unit of the Attorney General. Data collected by law enforcement authorities are:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and processed only in a manner compatible with these purposes;
- adequate, relevant and not excessive in relation to the purpose for which they are processed;
- accurate and updated where necessary;
- kept in a form that allows identification of the individual for no longer than is necessary for the purpose of the processing; and

- appropriately secured, including protection against unauthorised or unlawful processing, using appropriate technical or organisational measures.

Under Cyprus law, the Cypriot intelligence service can also access data, in the course of performing its duties. Any such access is subject to the requirements of the GDPR to the extent it concerns personal data.

Under certain circumstances, access to personal data by the authorities is subject to a requirement of prior court authorisation. This is the case where the access amounts to interception of private communications.

Any company that is a recipient of a request for information issued by the Police or the CIS is obliged to provide data to the authorities when presented with such request. With respect to orders for access to communications data, obliged entities include electronic communications service providers and electronic communications network providers.

Law stated - 28 September 2023

GAMING

Legality and regulation

Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

An online betting or gaming business is subject to authorisation by the National Betting Authority (NBA) of Cyprus. The NBA is the regulatory authority responsible for examining applications, licensing, auditing and supervising prospective betting shops and online betting operators in Cyprus. A particular licence may be granted by the NBA to authorise the provision of online betting services (excluding slot machines, online (live) casinos and online horseracing betting).

The following betting services, inter alia, are expressly prohibited in Cyprus:

- betting on horse races;
- limited betting games machines;
- spread betting; and
- betting on dog racing.

No one under the age of 18 can be registered to use online betting services offered under Cyprus law.

The following information must be obtained for the registration of a person to use online betting services offered under Cyprus law:

- confirmation that the player is over 18 years old;
- identification of the player;
- address of the player's residence;

- player's valid email address; and
- declaration that the player has been informed of the terms and the way of conducting the bet, including the remuneration that the player may potentially be called to provide.

Law stated - 28 September 2023

Cross-border gaming

Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

Under applicable Cyprus law, any person advertising online betting or gaming must not do so in a way that:

- implies that it promotes or relates to social acceptance, personal or economic success or the resolution of any personal, economic or social problems;
- involves the endorsement of well-known personalities in a manner that implies that it is related to their success;
- may in any way influence minors to participate in it;
- promotes its conduct by using services provided by a person who is not a licensee of a type provided for under the relevant legal framework, or an authorised representative; or
- exceeds the bounds of honesty and propriety.

Law stated - 28 September 2023

OUTSOURCING

Key legal issues

What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Outsourcing in non-regulated sectors is generally governed by the contractual arrangements concluded between the parties. If Cyprus law is the governing law of the outsourcing agreement, the following are some of the key considerations applicable to outsourcing relationships:

- liability and indemnity aspects;
- intellectual property rights that may reside in the software, equipment and documentation used for the outsourcing;
- intellectual property rights arising as a result of the outsourcing;
- compliance with processing of personal data requirements; and
- the applicability of the protection of employees' rights on transfers between undertakings.

Law stated - 28 September 2023

Sector-specific issues

Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

The Cypriot banking regulatory framework regulates outsourcing by credit institutions, namely agreements by which the service provider carries out a procedure, performs services or activities that would normally be undertaken, provided or exercised by the credit institution itself. Credit institutions are required to apply the European Banking Authority's Guidelines on outsourcing arrangements in relation to their outsourcing policy and processes.

A key aspect in outsourcing in the banking sector is that the credit institution that outsources any function always remains liable for compliance with its regulatory obligations and responsibilities towards its customers. Outsourcing by a credit institution entails varying reporting requirements (depending on whether a critical or important function is outsourced) and must contain specific contractual arrangements. Outsourcing must not hinder effective on-site or off-site supervision of the credit institution and shall not contravene any supervisory restrictions on services and activities.

In the financial and investment services sector, the European Securities and Markets Authority (ESMA) Guidelines on outsourcing to cloud service providers apply. Under the said guidelines, investment firms are required, among others, to:

- clearly assign responsibility for the documentation, management and control of cloud outsourcing arrangements;
- maintain sufficient resources to ensure compliance;
- adhere to specific requirements in respect of the outsourcing agreement when outsourcing critical or important functions;
- have a cloud outsourcing oversight function; and
- ensure that the cloud outsourcing written agreement does not limit the firm's and competent authority's effective exercise of the access and audit rights on the cloud service provider.

Insurance and re-insurance undertakings are subject to the European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers, which provide for similar requirements as the ESMA guidelines.

Law stated - 28 September 2023

Contractual terms

Does the law require any particular terms to be included in outsourcing contracts?

Sector-specific guidelines provide for specific terms to be included in outsourcing critical or important functions to a service provider. These guidelines include the European Banking

Authority's Guidelines on outsourcing arrangements in relation to their outsourcing policy and processes, the European Securities and Markets Authority Guidelines on outsourcing to cloud service providers and the European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers, all of which are applicable in Cyprus.

Indicative matters that must be governed under the terms of the agreement in sector-specific outsourcing of critical or important functions include:

- the time frame of the outsourcing;
- the governing law of the agreement;
- provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;
- agreed service levels that should include precise quantitative and qualitative performance targets for the outsourced function;
- reporting obligations of the service provider;
- taking out insurance;
- business continuity and contingency planning;
- locations; and
- exit and termination.

Law stated - 28 September 2023

Employee rights

What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Generally, outsourcing arrangements may be caught under the framework safeguarding employee rights in transfers of undertakings. Where this framework is found to apply, the transferor's rights and obligations as employer shall be transferred to the transferee undertaking. The transferor and transferee can agree that they shall be jointly and severally liable in respect of obligations that arose before the date of transfer from a contract of employment or an employment relationship existing on the date of the transfer.

The transferor and transferee have a duty to inform all affected employees of the transfer and related matters. The transferor or transferee (or both) may be required to consult with affected employees or their representatives when they envisage they will take measures in connection with the relevant transfer.

Law stated - 28 September 2023

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

In the personal data domain, data subjects have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects that concerns them or significantly affects them. This right is subject to limited exceptions and is protected with strict safeguards – including the right to obtain human intervention to data that are subject to automated decision making (including profiling).

An impact assessment is required in the event where there is systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing (including profiling) and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

In the wider artificial intelligence domain, the European Commission has tabled a proposal for a regulation on artificial intelligence (AI). The proposed regulation aims to ensure that AI systems placed on the EU market are safe and respect existing law on fundamental rights and EU values, ensure legal certainty to facilitate investment and innovation in AI, and facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

Law stated - 28 September 2023

IP rights

Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or machine learning systems?

Training data sets and software associated with artificial intelligence (AI) or machine learning may be protected by intellectual property rights, provided they meet the requisite originality requirements under applicable Cyprus law.

While Cyprus law does not expressly regulate intellectual property rights linked to AI, nor have such matters been tested in Cypriot courts, it is expected that AI-assisted works would be eligible to vest intellectual property rights to their creators. On the other hand, AI-generated creations would not be in a position to attract intellectual property right protection, as they would not meet the criterion of originality that is linked to a natural person and their personality.

Law stated - 28 September 2023

Ethics

Are there any rules or guidance relating to the ethics of artificial intelligence and machine learning?

Cyprus has developed guidance on ethics associated with AI or machine learning through the National Strategic Plan on AI which was developed by the Department of Electronic Communications of the Ministry of Transport, Communications and Works of the Republic of Cyprus (the DEC) in 2020 and is currently being implemented. This policy tackles matters on ethics associated with AI, including the need to protect the security, privacy and human rights of users and to ensure transparency on labelling requirements and traceability of AI software as well as the protection of the environment.

Law stated - 28 September 2023

TAXATION

Online sales
Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Income derived from trading in digital products and digital assets, including cryptoassets, is generally taxable. Profit achieved by companies in Cyprus is subject to a corporation tax of 12.5 per cent. Certain income may be tax deductible if the digital product concerned has been developed in Cyprus.

Cyprus entities' profit from qualifying IP assets may benefit from an 80 per cent tax deduction, resulting in an effective tax rate of 2.5 per cent or less. The regime, known as the 'IP Box', benefits software, patents, utility models and other intellectual property assets.

Law stated - 28 September 2023

Server placement
What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse-within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

The presence of servers in Cyprus or the operation of a metaverse out of Cyprus by a non-resident company does not in itself create tax residence in Cyprus, but may give rise to taxation depending on whether income is derived from such activity by a permanent establishment in Cyprus.

Law stated - 28 September 2023

Electronic invoicing
Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

Electronic invoices are equivalent to paper invoices under Cyprus law and businesses are free to issue electronic invoices subject to acceptance by the recipient. Cyprus law provides for mandatory electronic invoicing for all public procurement transactions (for both public and private suppliers). Copies of invoices, as part of the records kept in relation to a company's transactions in Cyprus, must be kept for a period of seven years.

Law stated - 28 September 2023

DISPUTE RESOLUTION

Venues

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

There are no special courts in Cyprus dealing with online or digital disputes. Any claim for breach of applicable law in relation to online or digital services, such as claims arising from breaches of the electronic commerce legislation can be dealt with by the Cypriot courts.

Online/digital issues and disputes primarily regarding consumers such as, inter alia, claims arising from e-commerce transactions, claims regarding delivery of damaged goods, unfair practices, goods that fail conformity requirements and surcharges can be resolved through dispute resolution bodies accessed via the Online Dispute Resolution (ODR) platform provided by the European Commission for the online resolution of disputes between consumers and traders.

The ODR platform can be used to submit a request that will then be notified to the trader. Depending on whether the trader is willing to address the request and resolve the dispute, the dispute may be resolved without further recourse to dispute resolution bodies. The consumer and trader should reach an agreement within a maximum of 90 days, at the lapse of which the consumer can address a dispute resolution body (which can be agreed with the trader) or pursue any remedies in court.

Law stated - 28 September 2023

ADR

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

A consumer has the choice of using ADR to resolve a dispute with a trader in respect of an online transaction.

Traders who agree or are obliged (in the case of a regulated sector) to use ADR must inform consumers accordingly on their websites as well as in their general terms and conditions. They must also inform consumers about ADR when a dispute cannot be settled directly between the consumer and the trader.

ADR bodies in Cyprus must have been approved by the competent authority. It is increasingly common in Cyprus for consumers to pursue the resolution of their dispute via ADR and for traders to agree to such dispute resolution process.

Law stated - 28 September 2023

UPDATE AND TRENDS

Key trends and developments

Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

Cyprus has several policy initiatives under implementation, which are expected to facilitate digital transformation, such as the Digital Strategy for Cyprus (2020–2025) and the Broadband Plan of Cyprus 2021–2025. EU instruments such as the Digital Markets Act and Digital Services Act are expected to have a major impact on business and transactions carried out online.

Law stated - 28 September 2023