

PANORAMIC

DIGITAL BUSINESS 2027

 LEXOLOGY

Digital Business 2027

Panoramic guide (formerly Getting the Deal Through) enabling side-by-side comparison of local insights into legal and regulatory framework; contracting on the internet; security, including security of payment; domain names; advertising; financial services; defamation; intellectual property; data protection; taxation; gambling; outsourcing; online publishing; dispute resolution; and recent trends.

Generated on: October 8, 2026

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2026 Law Business Research

Contents

Belgium

Steven De Schrijver

Allegiance Law

Chile

Claudio Magliona, Carlos Araya

Magliona Abogados

China

Jan Holthuis, Yongmei Evers Cai

BUREN

Germany

Franziska Ladiges, Matthias Orthwein, Stefan Peintinger, Johannes Schäufele, Daniel Meßmer

SKW Schwarz

Hungary

Endre Várady, János Tamás Varga

VJT & Partners

India

Hardeep Sachdeva, Priyamvada Shenoy, Shagun Badhwar, Nishant Thakur, Sahil Tandon, Amulya Bhatia

AZB & Partners

Italy

Paolo Balboni, Luca Bolognini, Raffaella Cesareo, Luciana Di Vito, Camilla Serraiotto, Claudio Partesotti

ICT Legal Consulting

Serbia

Jelena Hrle, Dragoljub Sretenovic, Tomislav Popović, Bogdan Ivanišević, Anja Gligorević

BDK Advokati

USA

Ieuan Jolly

Linklaters LLP

Belgium

Steven De Schrijver

Allegiance Law

Summary

LEGAL AND REGULATORY FRAMEWORK

Government approach
Legislation
Regulatory bodies
Jurisdiction
Establishing a business

CONTRACTING ON THE INTERNET

Contract formation
Applicable laws
Electronic signatures
Breach

FINANCIAL SERVICES

Regulation
Electronic money and digital assets
Digital and crypto wallets
Electronic payment systems
Online identity

DOMAIN NAMES AND URLS

Registration procedures
IP ownership

ADVERTISING

Regulation
Targeted advertising and online behavioural advertising
Misleading advertising
Restrictions
Direct email marketing

ONLINE PUBLISHING

Hosting liability
Content liability
Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

Belgium is a highly digitalised and modern country with many innovative businesses. It ranks high in the list of most innovative economies in the world and has one of the best digital infrastructures in Europe. The federal and regional governments support further growth of the technology sector with national and regional support strategies and plans on technologies such as artificial intelligence, Internet of Things, robotics and cybersecurity. There is a wide array of tax incentives and subsidies available for research and development and investment in innovation. Universities and other educational institutions also obtain important funding to provide support to digital businesses, train the next generation of technology specialists and conduct important research on technological developments. Digital business is, therefore, seen as a positive factor that strongly contributes to the economy and therefore its growth must be stimulated.

Law stated - 19 August 2026

Legislation

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

Given the broad impact of digital businesses and digital transformation in different sectors, it is difficult to pinpoint all the specific legislation that comes into play. The most important laws are the following:

- the Belgian Code of Economic Law;
- the (new and old) Belgian Civil Code;
- the Telecommunications Act of 13 June 2005;
- the Belgian Privacy Act of 30 July 2018 (implementing the General Data Protection Regulation where necessary); and
- the Belgian Act of 26 April 2024 establishing a framework for cybersecurity of network and information systems of general public safety interest (implementing the NIS2 Directive 2022/2555).

Law stated - 19 August 2026

Regulatory bodies

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

The most important regulatory bodies in the digital sphere are:

- Belgian Institute for Postal Services and Telecommunications (BIPT/IBPT) (telecommunications regulator);
- Federal Public Service Economy (FOD Economie/SPF Economie) (consumer and economic law regulator);
- Belgian Data Protection Authority (DPA) (Gegevensbeschermingsautoriteit/Autorité de protection des données);
- National Bank (Nationale Bank van België/Banque Nationale de Belgique) (financial services regulator); and
- Financial Markets and Services Authority (FSMA) (financial services regulator).

Law stated - 19 August 2026

Jurisdiction

- 4 | 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?

Under Regulation (EU) 1215/2012 of 12 December 2012 (Brussels I bis Regulation), a consumer may in principle bring proceedings against the digital business either in the home state of the digital business or in his or her own jurisdiction. On the other hand, a digital business may only bring proceedings against a consumer in the latter's home state. Where the customer is not a consumer, the parties may agree on a forum in their agreement or apply the other rules foreseen in the Brussels I bis Regulation.

Where disputes are held against a party outside the European Union, specific international private law rules will apply to determine the applicable jurisdiction. For example, Belgian courts have jurisdiction if the defendant is domiciled or habitually resident in Belgium when the claim is initiated, or if the parties have so agreed.

A party who finds that a dispute brought before a Belgian court should be brought somewhere else based on the underlying agreement, the Brussels I bis Regulation or other laws, must raise this in court. The Belgian court will in principle have to respect such rules, and in any case has to respect them when it comes to the Brussels I bis Regulation, save for a number of exceptions. The applicable law can be different to that of the applicable forum.

Law stated - 19 August 2026

Establishing a business

- 5 | 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?

No particularities apply to digital companies compared to 'normal' companies, and digital businesses can therefore be established in the same way. In principle, there is no authorisation or permit required to provide digital content and services, unless the company is operating in a regulated sector (eg, financial services or gambling).

Law stated - 19 August 2026

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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?

It is possible to form and conclude contracts digitally. The general formation rules of the Belgian Civil Code apply, namely, the parties must have the capacity to enter into an agreement, the valid consent of the parties is required, there must be a clear object and a lawful cause. A contract can be concluded digitally (eg, through a distance sale, email, etc). Additional rules may apply, especially in consumer contracts in distance sales, which among others require certain pre-contractual information obligations to be met and include mandatory post-sale rights such as a revocation of sale right. Belgian contract law also includes rules on unfair terms in both business-to-consumer (B2C) and business-to-business (B2B) relationships, some of them being null and void by law.

Law stated - 19 August 2026

Applicable laws

- 7 | 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?

Regulation (EU) 1215/2012 of 12 December 2012 (Brussels I bis Regulation) determines the courts before which a person may be called upon to appear in another member state. The law applicable to non-contractual obligations is determined by Regulation 864/2007/EC of 11 July 2007 (Rome II Regulation). The parties are in principle free to determine the forum and applicable law themselves, except in the case of specific agreements (eg, in a B2C relationship, an insurance agreement, etc) where restrictions apply.

While the parties are free to choose the language of the contract, the language used in specific contracts, such as in a B2C relationship, must be understandable and legible. To avoid the nullity of a contract with consumers, it is required that it be drafted in the language of the consumers, especially when it concerns complex services.

Law stated - 19 August 2026

Electronic signatures

- 8** | 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?

According to the Belgian Civil Code, a signature is valid when it consists of a sign or a succession of signs, affixed by hand, electronically or by any other process, by which a person identifies themselves and from which their expression of will appears. The Civil Code acknowledges that such a signature can be electronic.

A qualified electronic signature is recommended, in the sense of Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS Regulation), when applying a digital signature, rather than a scanned copy. Qualified electronic signatures can only be provided by a registered trust service provider, who is subject to a number of rules when providing an electronic signature service (especially in respect of consumers).

Law stated - 19 August 2026

Breach

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

No. Ordinary courts or arbitration institutes (eg, CEPANI in Belgium) will deal with such disputes.

Law stated - 19 August 2026

FINANCIAL SERVICES

Regulation

- 10** | 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?

The advertising or selling of financial services products to consumers or to business digitally is very strictly regulated. This includes rules in the Belgian Code of Economic Law and specific regulatory financial laws and may, for instance, include certain prohibitions on the type of advertising, the provision of comprehensive pre-contractual information or the provision of a cooling-off period during which the consumer can withdraw from the contract. Rules depend on the type of product, and will list in detail what information must be provided and which other obligations apply. General rules on unfair commercial practices may apply too. The supervisor of these rules is in principle the Financial Markets and Services Authority or the Federal Public Service Economy. When financial instruments are offered via the internet, the issuers thereof must also carefully verify whether or not the detailed rules on public offers, which are substantially based on European law, apply.

Law stated - 19 August 2026

Electronic money and digital assets

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

The Belgian Act of 11 March 2018 on the Legal Status and Supervision of Payment Institutions and Electronic Money Institutions, Access to the Business of Payment Service Provider and to the Activity of Issuing Electronic Money, and Access to Payment Systems, regulates the issue of electronic money, which is a licensed activity. Any person wishing to issue electronic money as an e-money institution in Belgium must, save for a number of limited exceptions, obtain a licence from the National Bank of Belgium. Book VII of the Belgian Code of Economic Law contains further rules on the issuing of e-money. A number of European regulations may also apply, as well as anti-money laundering regulations. Substantially the same rules apply throughout the European Union (EU).

Until recently, there were no specific rules applicable to digital assets and digital currencies. The only relevant instruments were the Belgian Anti-Money Laundering Act of 18 September 2017 and the Royal Decree of 8 February 2022, the providers of exchange services between fiat and virtual currency must register in Belgium. Providers of such services from outside the European Economic Area (EEA) are prohibited from providing their services in Belgium.

On 17 May 2023, the new Royal approving the Financial Markets and Services Authority (FSMA) regulation that imposes restrictive conditions on the commercialisation of virtual coins among consumers (FSMA Regulation) came into force. The FSMA Regulation intends to make consumers aware of the risks associated with virtual currencies and to regulate their promotion. The FSMA Regulation set forth several requirements, such as adhering to specific content guidelines to prevent misleading advertising. They mandate the inclusion of defined messages at the outset of advertisements, notably stating:

"Virtual currencies, real risks. The only guarantee in crypto is risk"

, along with a more detailed warning outlining the primary risks associated with investing in virtual currencies. Additionally, there is an obligation to inform the FSMA about all advertising in mass campaigns at least 10 days prior to distribution, in the exact format intended for dissemination.

Law stated - 19 August 2026

Digital and crypto wallets

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

The Belgian Anti-Money Laundering Act of 18 September 2017 regulates crypto exchanges and wallet providers. The new rules require providers engaged in exchange

services between virtual currencies and fiat currencies, as well as custodian wallet providers, to be registered in Belgium (including if they own ATMs in Belgium). Above all, they prohibit such providers from providing services in Belgium when they are established in a third country without having an establishment in the EEA. The Royal Decree of 8 February 2022 further details the registration conditions (eg, a fully deposited minimum registered capital of €50,000 and a fit and proper management). This is a unique Belgian law that is not found across all jurisdictions of the EU, and is for now separate from the rules under the adopted Markets in Crypto Assets (MiCA) Regulation which has entered into force on 30 December 2024. The transitional period under MiCA, during which existing providers could continue to operate under national rules, ended on 1 July 2026; since that date, all crypto-asset service providers active in Belgium must hold a MiCA authorisation. The Belgian Law of 11 December 2025 divides the authorisation and supervisory powers over crypto-asset service providers between the FSMA and the National Bank of Belgium.

Title I of the MiCA Regulation outlines its applicability to crypto-asset service providers and issuers, establishing uniform requirements for transparency and disclosure concerning issuance, operation, organisation, and governance of such providers. The regulation focuses on protecting consumers and preventing market abuse, specifically targeting crypto-assets that do not fall under existing EU financial services laws as financial instruments, deposits, or structured deposits. The MiCA Regulation identifies and covers three types of crypto-assets, namely asset-referenced tokens (ART), electronic money tokens (EMT), and other crypto-assets not covered by existing EU law. The legislation regulates issuance and trading of crypto-assets as well as the management of the underlying assets, where applicable, with additional regulatory rules aimed at 'significant' ART and EMT. The MiCA Regulation allows the Commission to issue delegated acts to adapt definitions to evolving market and technological trends. Titles II, III, and IV detail authorisation rules for various types of crypto-assets, requiring issuers to be legal entities incorporated within the EU, provide a detailed white paper outlining their operations, and comply with additional requirements specified in annexes accompanying the regulation. Title V sets out provisions on authorisation and operating conditions for crypto-asset service providers. Title VI sets prohibitions and requirements to prevent market abuse involving crypto-assets.

Law stated - 19 August 2026

Electronic payment systems

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

The Belgian Act of 11 March 2018 on the Legal Status and Supervision of Payment Institutions and Electronic Money Institutions, and the Code of Economic Law, contain the rules on electronic payment systems, implementing thereby the EU PSD2 framework into Belgian Law. Such payment institutions must be licensed in Belgium with the National Bank. The PSD2 framework regulates rules on third-party access to digital information in bank accounts, which may also be subject to the General Data Protection Regulation. Substantially the same rules apply throughout the EU.

As of 1 July 2022, all Belgian companies must offer consumers at least one way to pay electronically. This electronic payment cannot substitute the cash payment but must complement it.

Law stated - 19 August 2026

Online identity

- 14** | 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 Anti-Money Laundering Act of 18 September 2017 regulates AML requirements and is applicable to a long list of institutions, including financial institutions, providers of certain financial services and providers of gaming services. The Act is based on a risk-based approach that, depending on the customer, obliges organisations to apply different identification procedures before entering into a business relationship. Specific KYC rules may also apply in financial law based on the MiFID framework. Substantially the same rules apply throughout the European Union.

Law stated - 19 August 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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?

At international level, the non-profit organisation Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the management of domain names. A domain name must be requested from an authorised agent. At European level, several regulations govern the legal framework surrounding domain names with the .eu extension. EURid, a Belgian non-profit association with its head office in Brussels, takes care of the management. These domain names can only be requested by European Union (EU) citizens or persons or companies who have their residence or establishment within the EU. At national level, the Belgian Association for Internet Domain Name Registration (DNS Belgium) is only responsible for the management of domain names – not for requesting the domain name; that must be done through an authorised agent or ‘registrar’ who has entered into an agreement with DNS Belgium. The nationality of the party requesting the domain name is irrelevant, nor are there any other special restrictions. Foreign agents can request the registration of a domain name from DNS Belgium. Likewise, Belgian agents can address requests from Belgian and foreign customers to the relevant manager in another country.

It is interesting to note that the Belgian Data Protection Authority and DNS Belgium have concluded an agreement, dated 1 December 2020, pursuant to which certain restrictions can be placed on websites with a Belgian domain name that do not comply with the General Data Protection Regulation (GDPR), even possibly leading to a cancellation of the domain name. This procedure makes it possible to redirect .be domain names to a warning page of the government body that has the legal authority to act against serious breaches of certain rules of law. For instance, if the processing of personal data, via a website linked to the domain name, constitutes a violation of the GDPR, the Data Protection Authority can issue an order to freeze or stop that processing. Also, subsequently DNS Belgium can revoke the website linked to the .be domain name.

Law stated - 19 August 2026

IP ownership

- 16** | 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?

Strictly speaking, the applicant only receives a licence or exclusive right to use the domain name, but not the actual ownership. Nevertheless, a domain name holder can take action under the Code of Economic Law against another domain name holder if the domain names are similar or identical, subject to a number of conditions. Ownership of a trademark can also support a challenge against a similar domain name, as the owner can also invoke trademark law.

Law stated - 19 August 2026

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

At the European level, two key instruments govern online advertising: the Digital Services Act (DSA) and the Digital Markets Act (DMA).

The Digital Services Act, which came into force on 16 November 2022 and became applicable on 17 February 2024, regulates advertising on online platforms. It imposes several transparency obligations on providers of these platforms when posting advertisements. Specifically, providers must inform individual recipients about the entity on whose behalf the advertisement is presented and the main parameters used to determine the recipient. This information must be displayed in real-time with each advertisement. Additionally, providers of very large online platforms or search engines have an extra transparency obligation: they must create a public database disclosing all advertisements posted on their online interface for up to one year after their presentation. This database must include details about the advertiser, the intended audience, the disclosure period, and the number of advertisement impressions per market.

The Digital Markets Act, which came into force on 1 November 2020 and becomes applicable on 2 May 2023, applies specifically to ‘gatekeepers’—companies that have a significant impact on the internal market and meet two additional cumulative criteria. The DMA also establishes transparency obligations in online advertising. Gatekeepers are required to provide advertisers and publishers with clear pricing information upon request, on a daily basis, and free of charge. Furthermore, advertisers and publishers must have access to reliable and independent tools for measuring and verifying the performance of their advertising campaigns, also upon request and free of charge.

At the national level, the provisions of the Code of Economic Law apply (both in business-to-consumer and business-to-business relationships), since advertising is a commercial practice. For example, advertising is misleading if it displays false information or omits crucial information such that this induces the average consumer or business to make a decision about a transaction that the consumer or business would not otherwise have made. The rules on the permissibility of comparative advertising are also applicable. Comparative advertising is only permitted on condition that it:

- is not misleading;
- compares goods or services that meet the same needs or are intended for the same purpose;
- objectively compares one or more essential, relevant, verifiable and representative characteristics of these goods and services, which may include price;
- does not cause, among undertakings, the confusion of the advertiser with a competitor, or the confusion of brands, trade names, other distinguishing marks, goods or services of the advertiser with those of a competitor;
- does not damage the good name of or denigrate the brands, trade names, other distinguishing characteristics, goods, services, activities or circumstances of a competitor;
- for goods with a designation of origin, relates in any event to goods with the same designation;
- does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing mark of a competitor or of the designations of origin of competing goods; and
- does not present goods or services as an imitation or replica of goods or services bearing a protected trademark or trade name.

These are cumulative requirements. Therefore, advertising that does not comply with all conditions is prohibited. Furthermore, specific legislation may apply, such as in the case of advertising for medicine, financial services or alcohol.

In addition, Directive 2005/29/EC on Unfair Commercial Practices (UCPD) provides a horizontal, largely maximum-harmonisation framework for business-to-consumer advertising across all media, prohibiting misleading actions and omissions and aggressive practices, applying the average consumer and professional diligence tests, laying down a blacklist of practices that are always unfair, and imposing specific information duties for invitations to purchase. Complementing this in the business-to-business sphere, Directive 2006/114/EC on Misleading and Comparative Advertising (MCAD) prohibits

misleading advertising and sets the conditions under which comparative advertising is lawful—requiring objective, verifiable, like-for-like comparisons that are not misleading, do not cause confusion, denigrate, or take unfair advantage of competitors' marks or designations of origin—while enabling competitors and qualified bodies to seek injunctions and placing the burden on advertisers to substantiate claims. Both directives are transposed and enforced at national level and apply equally to online and offline advertising.

Publicity through electronic communication is also regulated in the Code of Economic Law, and may also be subject to the General Data Protection Regulation (GDPR) if it concerns the processing of personal data.

The Code of Economic Law also contains specific identification and transparency principles for online advertising.

Law stated - 19 August 2026

Targeted advertising and online behavioural advertising

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

At the European level, the Digital Services Act (DSA) and the Digital Markets Act (DMA) play crucial roles in regulating targeted and online behavioural advertising.

Firstly, the Digital Services Act bans targeted advertising if the provider of an online platform knows with reasonable certainty that the recipient is a minor. It also strengthens transparency obligations, ensuring that individuals targeted by such advertising understand why specific ads are shown to them. Furthermore, online platform providers are prohibited from using special categories of personal data (such as data on sexual orientation) for targeted advertising. For very large online platforms and search engines, information on why advertisements are shown must be available in a public database they create. These entities are also required to include the risks associated with targeted advertising in their annual risk assessment procedures.

The Digital Markets Act prohibits gatekeepers from tracking end users outside their core platform services for targeted advertising purposes without obtaining explicit consent. Additionally, the DMA mandates that gatekeepers conduct independent audits of their profiling techniques used in targeted and online behavioural advertising. The results of such an audit must be submitted to the Commission within six months after the gatekeeper's designation.

There are no specific regulations regarding targeted and online behavioural advertising in Belgium. These are subject to general rules on advertising and, if personal data is processed to analyse the user's behaviour, the GDPR. When cookies are used, which have a 'tracking' function that allows them to follow the browsing habits of internet users on other websites, prior consent to such use by the user must also be obtained following the provision of clear and precise information concerning the processing of the user's data. This applies regardless of whether the information is personal or anonymous. Consent is only not required if the cookies are used for the sole purpose of carrying out the transmission of a

communication or are strictly necessary to provide an information society service explicitly requested by the user.

Law stated - 19 August 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

The Digital Services Act introduces a ban on using 'dark patterns' on online platform interfaces. Dark patterns refer to user interface designs specifically crafted to deceive users into actions that are not in their best interest and often come at their expense. For example, a misleading advertisement claiming a product is the cheapest in the online shop because its best-before date is approaching, while other equivalent products are available at a lower price, would constitute a dark pattern in the context of misleading advertising.

The provisions of the Code of Economic Law regulate misleading advertising across all industries. Misleading advertising entails, among others, that false information is displayed or crucial information is omitted. Evidence must be provided that such information or omission of information induces the average consumer to make a decision about a transaction that he or she would not otherwise have made. In case of a misleading omission, the deception must relate to the essential information (eg, the main characteristics of the product, the price or the method of payment).

Law stated - 19 August 2026

Restrictions

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

The Digital Services Act (DSA) bans targeted advertisement to minors on online platforms. Where the provider of the online platform knows *with reasonable certainty* that a minor is using its platform, it must not offer targeted advertisements or use the minor's personal data for these purposes. Despite this requirement, there is no general obligation to verify users' ages across all websites, and the DSA explicitly states that online platforms are not required to collect additional personal data to determine users' ages. This creates a dilemma for platforms: they must avoid targeted ads for minors without collecting extra data, potentially leading them to cease targeted advertising altogether or rely on trusted third parties. While large platforms may already possess accurate age data, this ban applies universally to all online entities, including video game developers and e-commerce sites. Non-compliance can result in hefty fines under the DSA and GDPR, making adherence crucial. Companies must adopt a risk-based approach, assessing their audience and activity to determine the best strategy, especially if their services cater to minors.

Targeted advertisement on online platforms is also prohibited under the DSA when profiling uses special categories of personal data referred to in article 9(1) GDPR, such as ethnicity, political views, sexual orientation.

There are also specific restrictions for digital products and services with respect to financial services and gambling (the advertising of non-licensed gambling facilities and games being prohibited).

Law stated - 19 August 2026

Direct email marketing

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

The e-Privacy Directive has been implemented in the Code of Economic Law, which contains the opt-in principle for publicity. This means that the use of electronic communication for advertising is prohibited without the prior, free, specific and informed consent of the addressee. The GDPR may equally apply. Nevertheless, an exemption from consent applies in two situations.

- Firstly, by means of an entry in the customer file. This exception requires three conditions:
 - it must concern a real customer (this is a person with whom the service provider already had at least a contractual relationship) from whom the service provider received the electronic data directly, and not through third parties;
 - the service provider may only use the customer's electronic data for advertising purposes for similar products or services to those it offers; and
 - the service provider, at the time it receives the electronic data, allows the customer to object to such use free of charge and in a simple manner.
- Secondly, if the electronic message is sent to legal entities. It is irrelevant whether the legal entity is even a customer. However, two conditions apply:
 - the advertisement must be sent to a non-personal electronic address (eg, contact@firma.be), not to the address of an employee of a legal person; and
 - the products or services offered in the advertisement must be directed to legal entities – the advertising must not be intended for natural persons, as is the case regarding vacation destinations, for example.

Both the Belgian Data Protection Authority and the Federal Public Service Economy have issued detailed guidelines on direct marketing and publicity through electronic communications.

Law stated - 19 August 2026

ONLINE PUBLISHING

Hosting liability

22 |

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?

Under the Code of Economic Law, and pursuant to the EU Digital Services Act, three different types of exemptions of liability for providers of information society services exist when they act as intermediaries under the mere conduit principle. Generally speaking, when such providers do not initiate the transmission or do not have the opportunity to modify the information transmitted, they are exempted from liability. Specific conditions must be assessed for each type of exemption.

Law stated - 19 August 2026

Content liability

23 | 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?

There are no specific rules regarding liability for advertising and information published online. The general liability rules of the Civil Code, including those regarding the exemptions on liability through a disclaimer and its limitations, apply.

The Belgian Code of Economic Law provides for a cascading presumption of liability in the event of an action against publicity:

- the advertiser (if domiciled in Belgium);
- the publisher of the written advertising or the producer of the audio-visual advertising; the printer or the director; and
- the distributor.

Liability can be shared. Criminal liability is equally possible.

Law stated - 19 August 2026

Shutdown and takedown

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

While the Digital Services Act (DSA) reiterates the conditions under which intermediaries are exempt from liability, it also imposes new obligations to combat illegal content on their services. Illegal content is defined by EU and national laws, covering areas like intellectual property infringement, defamation, and hate speech. For example, the Belgian Supreme Court (Hof van Cassatie/Court de Cassation) did accept in 2013 that internet access providers can be required to make a website inaccessible to internet users. The purpose

of the data seizure is to stop acts that appear to constitute a crime. The data seizure is possible in two situations. Firstly, if the data constitutes the object of a crime or arose from a crime and is contrary to public order or morality; (criminal) hate speech and crimes always fall into this category, because of the broad wording. Secondly, if the data endangers the integrity of information systems or data stored, processed or transmitted by them.

Under the DSA, intermediary service providers (mere conduit, caching and hosting) are required to implement the following:

- **Notification Mechanisms:** Intermediaries must implement an accessible and user-friendly process for individuals or entities to notify them of illegal content. Notices must be precise and substantiated, including reasons for illegality, the content's location (eg, URLs), the reporter's name and email, and a good faith statement. Once notified, intermediaries are liable if they do not promptly remove or disable access to the illegal content.
- **Communication Obligations:** Intermediaries must acknowledge receipt of the notice and inform the reporter and the affected party of any actions taken, including reasons for removal or disablement of content.
- **Appeal Mechanisms:** Intermediaries must provide an appeals process for at least six months for decisions related to content removal, service suspension, or account termination. These appeals cannot be resolved solely by automated means and must involve human review.
- **Repeat Abuse Policies:** Service providers can suspend users who frequently provide illegal content or abuse the notification system. Their terms and conditions must outline their policy on repeated abuse, including factors for assessing misuse and suspension durations.

Although the DSA does not require intermediaries to monitor or actively investigate illegal activity, it mandates the establishment of notification and appeal mechanisms, expanding beyond the scope of the e-Commerce Directive. Non-compliance can result in penalties up to 6 per cent of annual income or turnover, making it crucial for service providers to implement the required infrastructure to meet these obligations.

Law stated - 19 August 2026

INTELLECTUAL PROPERTY

Data and databases

25 | Are data and databases protected by IP rights?

It is generally accepted that data are not protected by intellectual property rights. After all, there is no creative process happening with data as there is in relation to copyright. However, this view needs to be nuanced. For example, it is possible that the selection and arrangement of data take place in a certain way for which creative choices have been made. In such a case, one can claim copyright on the structure of the database.

Databases, on the other hand, are protected by intellectual property rights, specifically by the Code of Economic Law. These can be protected by:

- a specific sui generis right, protecting the content of the database, even if it is not original, and certain conditions (eg, sufficient investments were made); and/or
- copyright law protecting the structure of the database, if it is original.

Law stated - 19 August 2026

Third-party links and content

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

In principle, it is permitted to link to a third-party website. However, liabilities arise if a link is made to unlawful content. Restrictions may also apply if content is embedded in a webpage by means of hyperlinks and frames wherein third-party content is displayed. Under European Union copyright law, it is permissible to hyperlink to a website of a third party if the linked material is: (1) still publicly available; and (2) was originally communicated on the internet with the content owner. The link may be infringing a third-party copyright if the linked material has been removed or if it circumvents any subscription, pay or other technical barriers imposed by the original content owner.

Law stated - 19 August 2026

- 27** | 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?

Yes, unless such content is protected by copyright laws or if it contains personal data, in which case the obligations under the General Data Protection Regulation apply. Scraping could also be prohibited based on a website's terms of use.

Law stated - 19 August 2026

Metaverse and online platforms

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

Novel technologies often give rise to novel legal issues, as the law is usually behind technological developments. The metaverse is not different in this sense. Examples thereof are the questions regarding the creation and protection of intellectual property rights for downloadable virtual goods and services in the metaverse, and the scope of the rights to use the content held by a non-fungible token owner (eg, with respect to the classification and similarity of goods and services and the doctrine of exhaustion).

The European law prescribes that trademarks can still be asked for the products created in the metaverse. Since such products are just considered to be a virtual appearance of real products, one shall indicate in a trademark application for them the same class as the one under which their 'normal' equivalent falls.

In *Bezpečnostní softwarová asociace* case the CJEU came to the conclusion that the creations of graphical user interfaces made in the metaverse can be considered as artistic works. In this regard, they can be protected by copyright as long as such graphical user interface is the own intellectual creation of an author.

Law stated - 19 August 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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?

The first-sale doctrine is recognised under European law and requires a first sale that occurred with the consent of the right holder within the European Economic Area. The Court of Justice of the European Union stated that a sale may involve tangible and intangible property. Consequently, for digital products, one can speak of a 'first-download doctrine'.

The question of whether the rights can be exhausted by placing the digital product on a metaverse is still disputable. In this regard, it looks like that the answer for it is negative. In conformity with the EU law, the principle of exhaustion of rights is mostly applicable to the restriction of distribution rights. Based on the implications of the *Tom Kabinet* case, the EU distribution rights seem to be applicable to tangible goods only, while the products on a metaverse are, in essence, in intangible form. The same logic applies even if such a product itself is representative of the digital work. However, there is no case law yet, which directly confirms or rejects this theory.

Law stated - 19 August 2026

Administrative enforcement

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

The General Directorate of Economic Inspection has several tasks, listed in the Code of Economic Law. One of its roles is to monitor compliance with economic regulations through informative, preventive, warning and repressive action. This includes detecting and determining violations of the Code of Economic Law and various economic regulations. For example, the Directorate can carry out dawn raids and seize false products that infringe intellectual property rights.

Law stated - 19 August 2026

Civil remedies

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

The IP owner can file a cease-and-desist action in a civil court to order the cessation of an infringement of IP rights. The cessation may be accompanied by a penalty payment. The owner may also seek damages to compensate them for their loss. Furthermore, they can request measures for the description and preservation of any infringing material. This procedure is called 'the seizure of counterfeit'. Finally, certain ancillary claims are possible, such as for the remittance of profits, the recall of the goods from the market or the forfeiture of the infringing goods.

Law stated - 19 August 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

- 32** | 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?

Under the General Data Protection Regulation (GDPR), 'personal data' means any information relating to an identified or identifiable natural person whereby an 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition applies throughout the European Union (EU).

Additionally, a number of categories of sensitive personal data exist (eg, data about a person's health, ethnicity, sexual orientation or political views). The processing of these data is prohibited, barring exceptions. For example, if the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, or if the processing relates to personal data that are manifestly made public by the data subject.

Law stated - 19 August 2026

Registration and appointment of data protection officer

- 33** | 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?

There is no registration requirement to be allowed to process personal data. However, any organisation processing personal data must have a valid legal basis to do so. There are six legal bases listed in the GDPR:

- consent;
- performance of a contract;
- legitimate interest;
- vital interest;
- legal requirement; and
- public interest.

Each legal basis is subject to a number of conditions that have to be carefully assessed. Further obligations apply under the GDPR, including the requirement to document all activities concerning the processing of personal data in the data register.

The GDPR prescribes the appointment of a data protection officer (DPO) in three cases: (1) if there is a large-scale regular and systematic monitoring of users; (2) if the processing is carried out by a public authority; and (3) if the organisation is performing complex operations with user data. If the organisation falls outside one of these cases, the appointment of a DPO is not mandatory, but allowed voluntarily.

Law stated - 19 August 2026

Extraterritorial issues

- 34** | 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 is applicable in the three following situations:

- the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not;
- the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:
 - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
 - the monitoring of their behaviour as far as their behaviour takes place within the EU.
- the processing of personal data by a controller not established in the EU, but in a place where member state law applies by virtue of public international law.

Nevertheless, data controllers or processors that are not based in the EU but perform processing activities that fall within the scope of the GDPR, must designate a representative in the EU.

Law stated - 19 August 2026

Bases for processing

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

There are six legal bases for processing listed under the GDPR:

- consent;
- performance of a contract;
- legitimate interest of the data controller;
- vital interests;
- legal requirement; and
- public interest.

Each of them is subject to its own rules and conditions. A sufficient legal basis must be established to export personal data to a jurisdiction outside the EU, to which additional obligations apply.

Law stated - 19 August 2026

Data export and data sovereignty

36 | 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?

Cross-border data transfers within the European Economic Area or to countries that are considered to provide adequate data protection in comparison to the EU are permitted. An adequate level of protection is provided through a European Commission adequacy decision. A transfer outside the EU is then equated with a transfer within the EU. The countries that benefit from the adequacy decision are, currently, the United States (commercial organisations participating in the EU-US Data Privacy Framework) Andorra, Argentina, Canada (for commercial organisation), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.

In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Examples of safeguards

are the use of binding corporate rules, (the 'new') standard contractual clauses (SCCs) (taking into account the European Court of Justice's Schrems II judgment) and adherence to other formalities. The Schrems II judgment states that the US does not provide an adequate degree of protection due to a lack of proportionality of mass- surveillance programmes and a lack of effective remedies equivalent to those required by the GDPR. Therefore, the EU- US Privacy Shield adequacy decision is invalid, which means that it can no longer be relied on to transfer personal data to the US. However, the EU and the United States have negotiated a new framework to address the requirements of Schrems II. Adopted in July 2023, this framework applies exclusively to commercial organisations participating in the EU-US Data Privacy Framework.

If there is no adequacy decision and no safeguards, a transfer can be made based on a limited number of derogations for specific situations. For example, it may be sufficient that an individual, who is aware of all the risks of the transfer, explicitly agrees to such data transfer.

Law stated - 19 August 2026

Sale of data to third parties

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

The two most generally accepted legal bases in the GDPR for the sale, license or transfer of personal data are the data subject's consent and the data controller's legitimate interests. If the data is sold or transferred without a legal basis for the processing, it must be deleted by the purchaser. The seller can be held liable for the sale price and any damages in case of an illicit transfer.

Law stated - 19 August 2026

Consumer redress

- 38** | 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?

Data subjects have multiple rights and remedies under the GDPR. For instance, they have the right to lodge a complaint with a supervisory authority (the Data Protection Authority), the right to an effective judicial remedy against a controller/processor/supervisory authority and the right to compensation and liability. Specifically in Belgian law, they can invoke article 1382 of the (Old) Civil Code to hold another party liable for infringements of the GDPR and the Belgian Privacy Act of 30 July 2018.

Law stated - 19 August 2026

Non-personal data

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

Yes, although the framework is predominantly of EU origin and considerably lighter than the regime for personal data. The Free Flow of Non-Personal Data Regulation (EU) 2018/1807 applies directly in Belgium and prohibits unjustified data-localisation requirements, guaranteeing that non-personal data may be stored and processed anywhere in the Union. A small number of Belgian localisation rules survive on public-interest grounds: books and records must remain at the disposal of the Belgian tax administration under article 315 of the Income Tax Code, and certain social and employment documents must be kept in Belgium and available on site under the Royal Decree of 8 August 1980.

The EU Data Act (Regulation (EU) 2023/2854), applicable since 12 September 2025, is now the centrepiece of non-personal data regulation. It grants users of connected products and related services (including businesses operating IoT devices) rights of access to the data those products generate, requires data holders to share such data with third parties designated by the user on fair, reasonable and non-discriminatory terms, prohibits unfair contractual terms in data-sharing contracts, facilitates switching between cloud and edge providers, and restricts international governmental access to non-personal data held in the EU. The Data Governance Act (Regulation (EU) 2022/868) governs the re-use of protected public-sector data, data-intermediation services and data altruism; Belgium implemented it through the Act of 15 May 2024 and the Royal Decree of 1 October 2024, which include redress procedures for data re-use requests. Open data held by Belgian public bodies is separately governed by the federal and regional transpositions of the Open Data Directive (EU) 2019/1024.

General Belgian law also shapes the use of non-personal data: the Code of Economic Law protects databases through the sui generis database right and implements the Trade Secrets Directive, while contract law remains the primary instrument for allocating rights in industrial and machine-generated data. Finally, mixed datasets require care — where non-personal data is inextricably linked with personal data, the GDPR applies to the entire set, so the boundary between the two regimes must be assessed case by case.

Law stated - 19 August 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

In principle, most documents and archives can be held digitally, provided that the authenticity of the digital copy can be proven to the authorities when required.

Law stated - 19 August 2026

Retention

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

Different retention periods apply to different types of documents. These range, for the most important categories, from five years following the completion of the liquidation of a company for corporate documents to 10 years for the accounting documents. Invoices must be kept for seven years. Documents with respect to the employment of personnel must usually be kept for five years.

Law stated - 19 August 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

Under the General Data Protection Regulation (GDPR), organisations must take appropriate technical and organisational measures to protect their processing of personal data, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity of these risks to potentially infringe the rights and freedoms of natural persons.

The Belgian Act of 26 April 2024 establishing a framework for cybersecurity of network and information systems of general interest for public security, transposes the EU Directive 2022/2555, known as the NIS2 Act, which replaces the NIS1 Directive (Directive (EU) 2016/1148). Published in the Belgian Official Gazette on 17 May 2024, the Belgian NIS2 Act will come into force on 18 October 2024.

The NIS2 Act mandates twelve additional sectors to implement cybersecurity risk management measures and follow incident notification obligations. It enhances and streamlines security and reporting requirements by establishing a minimum list of key elements all entities must consider, including incident management, supply chain security, and vulnerability handling and disclosure.

- The law applies to operators of essential services such as energy, drinking water, wastewater, transportation, banking, health, space, financial markets, ICT service management, governments, and digital providers like Internet nodes, DNS service providers, TLD name registries, cloud computing service providers, data centers, content delivery networks, trust service providers, and public electronic communication networks and services.
- It also covers important services, including postal and courier services, waste management, accounting firms, online marketplaces, search engines, social networking platforms, research organisations (excluding education), chemical

production and distribution, wholesale and industrial food production and processing, and manufacturers of medical devices, electrical equipment, motor vehicles, trailers, semi-trailers, machinery, and equipment.

Organisations in these sectors must meet certain size thresholds (employee headcount and annual turnover) to be covered by NIS2. They are subject to strict cybersecurity risk management requirements, including implementing risk analysis policies, proper incident handling, auditing, testing, and cybersecurity supply chain due diligence. The rules on incident notification have also been tightened.

Belgium has expanded the list of risk management measures and information obligations. Entities under the Belgian NIS2 law must adopt a coordinated vulnerability disclosure policy and conduct comprehensive risk analysis to safeguard networks, information systems, and physical environments. Based on this assessment, they must develop a security policy for information systems and networks, incorporating legally stipulated elements. This list of obligations can be extended by royal decree.

The NIS2 Act imposes higher cybersecurity standards and includes data protection and breach procedures, covering more than just personal data, unlike the GDPR. The national regulator can issue binding injunctions and administrative fines of up to €10 million or 2 per cent of the annual worldwide turnover (whichever is higher) for essential entities and up to €7 million or 1.4 per cent for important entities. Directors and management bodies are also liable for non-compliance, as they are responsible for implementing the required measures and must undergo appropriate cybersecurity training.

Law stated - 19 August 2026

Data breach notification

- 43** | 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?

With respect to data breach notifications, the Electronic Communications Act of 13 June 2005 requires companies in the telecommunications sector to notify immediately (within 24 hours) personal data breaches to the Data Protection Authority (DPA), which must transmit a copy of the notification to the Belgian Institute for Postal Services and Telecommunications. If there is a breach of personal data or the privacy of individuals, the company must also notify the data subjects affected by the breach. The NIS2 Act additionally provides for a detailed procedure regarding breaches for operators of essential and important services.

The GDPR provides for a duty for the data controller to report personal data breaches to the DPA without undue delay, and where feasible, not later than 72 hours after having become aware of a breach. This notification must describe the nature of the breach, communicate the contact details of the data protection officer or other contacts where more information can be obtained, explain the likely consequences of the breach and describe the measures taken or proposed to be taken by the controller to address the breach. A communication to the data subjects is in some cases necessary if there is a high risk to their rights and

freedoms. The DPA stresses that, in the event of public incidents, it must be informed of the causes and damage within 48 hours after the data controller became aware of the breach.

Law stated - 19 August 2026

Government interception

44 | 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?

Article 46 bis of the Code of Criminal Procedure provides that the Public Prosecutor, in the detection of crimes and malpractices, may, by a reasoned and written decision, on the basis of any data in his or her possession or by means of access to the customer files of the actors, proceed to:

- the identification of the subscriber or habitual user of a service, or of the electronic means of communication used; and
- the identification of the services subscribed to or habitually used by that person.

To this end, the Public Prosecutor may, if necessary, issue a request through a police department or the Federal Computer Crime Unit. He or she may also request the cooperation of the operator of an electronic communications network.

Article 88 bis states that the investigating judge, when there are serious indications that the offences may result in a correctional punishment of one year or a more severe punishment, and when he or she considers that there are circumstances that make it necessary to have electronic communications traced or to locate the origin or destination of electronic communications in order to uncover the truth, can:

- cause the traffic data of electronic means of communication, from which or to which electronic communications are or were made, to be traced (essentially the IP addresses); and
- have the origin or destination of electronic communications traced.

A number of additional legal grounds on lawful access to data exist, including for the secret services in the Act of 30 November 1998 Governing the Intelligence and Security Services. One more important example concerns the lawful access to personal data with the aims of prevention, detection, and prosecution of crimes in the Belgian Privacy Act, including prevention and protection against the threat to public safety.

Law stated - 19 August 2026

GAMING

Legality and regulation

45 | 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?

Belgium has a 'system of additional licences'. Only existing gaming establishments already licensed to operate games of chance in the real world (offline) can apply for an additional licence for the internet (online). Gambling is strictly regulated.

The Gambling Act requires a minimum age of 21 to play in a casino or slot machine hall, both offline and online. In addition, you are required to register for this purpose. To participate in either offline or online betting, the minimum age is 18. Certain professions are prohibited from accessing casinos and gaming arcades, for example magistrates. Also, certain persons can be placed in a database of excluded persons that must be consulted by gambling businesses before allowing customers to play. Online gambling businesses must impose compulsory game limits and include the possibility of temporary self-exclusion for customers, who must also be informed of the risks of online betting. Credit cards cannot be used to pay for online gambling services, nor can any credit or loan be provided.

Law stated - 19 August 2026

Cross-border gaming

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

Member states of the EU are free to define the level of protection on games of chance, as long as their national legislation complies with European law. They can restrict the cross-border supply of online gambling services on the basis of public interest objectives that they seek to protect (eg, fighting fraud). Therefore, the exclusion of online gaming providers located in other member states is not a restriction on the free movement of services. The provision and use of the cross-border gambling offer falls within the scope of the fundamental freedoms of the Treaty on the Functioning of the European Union. A Belgian gambling licence will therefore rarely provide the possibility to provide services in another European Union member state.

Law stated - 19 August 2026

OUTSOURCING

Key legal issues

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

Since the pandemic, the outsourcing of cloud computing services has boomed in Belgium. One of the most important concerns in this field remains privacy and cybersecurity, which must be extensively addressed in the outsourcing agreement. This is also necessary in other outsourced activities. If services are outsourced outside Belgium, and especially outside the European Union, the strict European rules on personal data transfers are likely to apply and cause issues that need to be addressed in a data processing agreement. Another crucial negotiation subject is an adequate service level agreement,

which guarantees that the provider will sufficiently support the customer's outsourced services. If personnel are to be transferred together with the outsourcing, it is essential to obtain advice on the Belgian employment law in this area, as such transfers are strictly regulated, among others pursuant to the European Acquired Rights Directive. The customer must also pay attention to the exclusions and limitations of liability clauses in the outsourcing agreement. The inclusion of common law terminology such as 'indirect damages' does not correspond with Belgian law, which has separate rules on liability that must be carefully transposed in the agreement. The parties must also think of the exit arrangements, as a lack of them can cause major issues for the customer when the agreement is terminated for any reason.

Law stated - 19 August 2026

Sector-specific issues

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

There are no specific regulations that would prohibit the outsourcing of digital business services. There are, however, specific rules on the outsourcing of activities by financial institutions and insurance companies that must be adhered to. For instance, the Act of 25 April 2014 on the Status and Supervision of Credit Institutions and Listed Companies states that the financial sector must take appropriate measures to limit the risks of outsourcing. Further European and national regulatory guidelines on outsourcing may apply in the financial sector.

Law stated - 19 August 2026

Contractual terms

- 49** | Does the law require any particular terms to be included in outsourcing contracts?

Belgian law does not prescribe any specific terms for an outsourcing agreement, as the main principle is contractual freedom subject to the general rules of the Belgian Civil Code and the Code of Economic Law.

Law stated - 19 August 2026

Employee rights

- 50** | 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?

If a service is outsourced, there may be circumstances in which the EU directive on Transfers of Undertakings with Protection of Employment (TUPE) applies, namely, the

Acquired Rights Directive (ARD). In Belgium, the ARD is incorporated by the Act of 5 December 1968 on Collective Bargaining Agreements and by the Collective Bargaining Agreement No. 32 bis (CBA 32 bis), which may apply if an asset and employee transfer takes place at the moment of the initial outsourcing, or if there is a change of supplier or a reverse transfer.

Belgian law will apply to any employee who usually executes their contract in Belgium, even if they are temporarily seconded to another country. If an employee does not execute their contract in one single country, the law of the country in which the employer is situated will apply.

All employees connected to the outsourced (transferred) activity must transfer, and will do so automatically, so that no new employment agreement is required with their new employer. A dismissal due to the transfer of undertaking is only possible for economic or technical reasons. Infringement may lead to additional compensation being due to the employees who were wrongfully dismissed.

The employer (transferor) must inform and consult its works council prior to making any official decision on an outsourcing that results in a transfer of employees. The works council must be informed regarding the reasons for the contemplated outsourcing and the consequences for the employees. There is only a duty to consult the works council, its consent is not required. The new employer (transferee) must also inform and consult its works council beforehand. Failing to inform and consult the works council can be sanctioned by a criminal fine.

If no works council (or trade union delegation) exists within the transferor, the employees concerned must be individually informed beforehand of the envisaged transfer date, the reasons for the transfer, the legal, economic and social consequences, and the intended measures that will affect the employees. In practice, the customer and the service provider will in most cases agree on a joint communication.

Law stated - 19 August 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

Attention should be paid to the European Union's Regulation 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence, commonly known as the EU AI Act. This regulation aims to harmonise rules on artificial intelligence, emphasising ethics and European values to foster the responsible development and use of AI technology. Adopted on 13 June 2024, the AI Act entered into force on 1 August 2024, with a phased implementation schedule:

- From 2 February 2025: Prohibitions on AI systems presenting unacceptable risks.

- From 2 August 2025: Rules concerning general-purpose AI models came into effect, along with the designation of competent authorities in Member States. The General-Purpose AI Code of Practice, published in July 2025, assists providers in demonstrating compliance with these obligations.
- From 2 August 2026: All other provisions, except those for high-risk AI systems, apply, including the transparency obligations of article 50 of the AI Act. Generative AI systems already placed on the market before 2 August 2026 benefit from a grace period until 2 December 2026 to comply with the machine-readable marking (watermarking) requirements.
- Following the 'Digital Omnibus on AI' adopted by the EU legislator in June 2026, which amends the AI Act, the rules for stand-alone high-risk AI systems listed in Annex III will apply from 2 December 2027, and the rules for high-risk AI systems embedded in regulated products listed in Annex I from 2 August 2028 (instead of 2 August 2026 and 2 August 2027, respectively). The Digital Omnibus also postpones the deadline for Member States to establish at least one national AI regulatory sandbox to 2 August 2027 and introduces a new prohibition, applicable from 2 December 2026, on AI systems used to generate non-consensual intimate images or child sexual abuse material.

Compliance with the AI Act varies based on the risk level posed by AI systems, determining specific obligations for providers and users. The Act categorises AI systems into four risk levels:

- **Unacceptable Risk Level:** AI systems that violate EU fundamental rights and values are fully prohibited.
- **High-Risk Level:** AI systems impacting health, safety, and fundamental rights are permitted but must meet additional obligations. Providers must conduct conformity assessments, establish risk management systems, adhere to data governance requirements, maintain technical documentation, keep records, and provide information to deployers.
- **Transparency Risk Level:** AI systems at risk of impersonation, manipulation, or deception are subject to specific information and transparency requirements.
- **Minimal Risk Level:** Common AI systems posing minimal risks to safety, health, and fundamental rights have no specific obligations or regulations.

In the EU AI Act, a fundamental rights impact assessment (FRIA) is mandatory for certain high-risk AI systems, such as those used by public bodies, private entities providing public services, or for evaluating creditworthiness and insurance risks. The FRIA requires identifying and mitigating risks to fundamental rights listed in the EU Charter, like non-discrimination and data protection. Although it mainly applies to high-risk AI systems, private entities providing public services may also be affected. The FRIA must be conducted before deploying a high-risk AI system and updated regularly. It includes a detailed description of the AI system, an assessment of potential harms, and proposed risk mitigation measures. It should involve stakeholder consultation and be integrated into the AI system's development phase.

Additionally, FRIA processes can overlap with GDPR's DPIA, and both assessments may be combined into a single report. Article 22 of the General Data Protection Regulation

(GDPR) gives data subjects the right not to be subject to a decision based solely on automated processing if such processing will lead to a decision that produces legal effects or has a significant impact on the data subject. Data subjects have the right to request that the decision be reviewed by a human. Additionally, under Belgian law, the Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data prohibits a person from being made subject to the legal consequences of a decision that was taken based on automatic processing of personal data evaluating certain aspects of a person's personality.

Moreover, AI should be transparent to meet the principle of transparency under articles 13 to 15 of the GDPR. The data subject should know that automated decision-making (including profiling) exists in the processing of its data and, in such case, must receive meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. Evidently, the AI systems themselves should also be designed in a way that secures processing of data and which only allows processing that is necessary for the organisation's legitimate goals.

Law stated - 19 August 2026

IP rights

- 52** | 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?

It depends on the type of data that are being used to train machine learning-based systems. Personal data will belong to the data subject and cannot thus be owned by, for instance, a developer of AI systems. The GDPR must be respected for any use of such personal data. A database containing personal data, in contrast, could enjoy protection by either or both of the following: (1) a specific *sui generis* right, protecting the content of the database, even if it is not original, and subject to a number of strict conditions; (2) copyright law protecting the structure of the database, if it is original.

Non-personal data can be owned and licensed contractually. Recent legislation, including the Data Governance Act (effective from 23 June 2023) and the Data Act (in force since 11 January 2024 and applicable since 12 September 2025), promotes and in some cases mandates data sharing for altruistic purposes. The challenge arises with copyright-protected works used to train machine learning systems, an issue that has gained prominence with the rise of Generative AI technologies like ChatGPT, which rely on such data for training. The Directive on Copyright in the Digital Single Market (DSM) provides some clarity. In Belgium, this Directive is implemented through the Act of 19 June 2022, effective from 1 August 2022. According to the DSM Directive, copyright-protected works can be lawfully used for training Generative AI for scientific research. They can also be used for other purposes unless specifically reserved by the copyright holder. However, determining whether such a reservation exists can be challenging in practice.

A work created by AI does not meet the current conditions for copyright protection. After all, no creative choices are made by the system. Also, the European Patent Office has rejected patent applications based on inventions with an AI system as inventor, as the latter should have a family name and thus be a natural person.

Law stated - 19 August 2026

Ethics

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

Belgium has not adopted a dedicated national AI statute; the governing framework is the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which applies directly in Belgium and is being phased in, with prohibitions on unacceptable-risk practices and AI-literacy obligations applicable since February 2025, obligations for general-purpose AI models since August 2025, and the bulk of the high-risk regime applying from August 2026. The AI Act itself embeds ethical requirements — human oversight, transparency, non-discrimination, accuracy and robustness (that were derived from the EU High-Level Expert Group's Ethics Guidelines for Trustworthy AI). At national level, the 2025–2029 Federal Government Agreement designates the Belgian Institute for Postal Services and Telecommunications (BIPT) as the principal market surveillance authority under the AI Act, alongside a granular list of specific bodies competent for high-risk systems affecting fundamental rights.

Beyond binding legislation, several soft-law instruments address AI ethics. The federal SmartAI.Nation convergence plan promotes trustworthy, human-centric AI aligned with the OECD AI Principles, building on the AI4Belgium coalition, which has issued policy recommendations on responsible AI since 2019. A federal advisory committee on data ethics and AI provides non-binding ethical guidance for the federal administration. Regionally, the Flemish AI Policy Plan 2024–2028 dedicates a pillar to ethics and societal awareness (supported by the Knowledge Centre Data & Society), while Brussels pursues responsible AI through the FARI institute and Wallonia through DigitalWallonia4.ai.

Sectoral regulators also contribute: the Belgian Data Protection Authority has published guidance on AI systems and the GDPR from a data-protection perspective, which is particularly relevant given that automated decision-making and profiling under article 22 GDPR remain key constraints on machine-learning applications. The National Bank of Belgium and the FSMA follow European supervisory authorities' expectations on AI governance in financial services. Practitioners should also note existing rules with ethical dimensions that apply to AI outputs, including anti-discrimination legislation, consumer-protection rules on unfair commercial practices, and product-liability rules as modernised by the new EU Product Liability Directive, which expressly covers software and AI systems.

Law stated - 19 August 2026

TAXATION

Online sales

- 54** | Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

A sales tax rate (VAT) of 0 per cent, 6 per cent, 12 per cent and 21 per cent applies in Belgium, depending on the product. The applicable rate for digital products and services is in principle 21 per cent. Income from digital products (such as speculation on tokens and crypto currency) may be taxed at 33 per cent on gains made, depending on the circumstances.

Law stated - 19 August 2026

Server placement

- 55** | 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 relevant criterion to determine whether or not a foreign company is active in Belgium depends on whether the activity concerned (such as placing a server, platform or metaverse) in Belgium can be seen as a 'permanent establishment'. The US concept of 'being engaged in trade or business' does not apply. The term 'permanent establishment' will depend on the circumstances of the activity and on the definition provided in the tax treaty between Belgium and the country of the foreign entity, if available. Generally, this is defined as the fixed place of business through which the business of an enterprise is wholly or partially carried on.

Law stated - 19 August 2026

Electronic invoicing

- 56** | 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?

The content of an invoice is regulated by law, which also applies to electronic invoices. E-invoicing is mandatory for domestic business-to-business transactions between Belgian VAT-taxable persons since 1 January 2026. Structured electronic invoices complying with the European standard EN 16931 (Peppol BIS format) must in principle be exchanged via the Peppol network, and a paper invoice or a PDF invoice sent by email is no longer sufficient in such relationships. An administrative tolerance period applied during the first three months of 2026, and failure to have the technical means to issue and receive structured electronic invoices is now sanctioned with fixed fines of up to €5,000. A near real-time e-reporting obligation for invoice data is expected to follow by 2028. Outside the scope of this mandate (eg, in business-to-consumer relationships), e-invoicing remains

permitted provided that the customer agrees to receive the invoice electronically. It must further be made sure that the electronic invoice is authentic, readable and the integrity of its content is maintained. It is also important to take Belgian language rules into account: the invoice must be provided in the language of the region in which the company's seat is located (Dutch in Flanders, French in Wallonia, Dutch or French in Brussels). This language must also be maintained if an invoice is provided to another region within Belgium or outside the European Economic Area. Within the European Economic Area, a copy of the local invoice in another language will also be declared valid. In practice, multilingual invoices are often used.

Copies of the invoices need not be provided to the tax authority or other agency on a regular basis, but must be kept for at least ten years to remain available during tax inspections.

Law stated - 19 August 2026

DISPUTE RESOLUTION

Venues

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

No, ordinary courts or arbitration institutes (CEPANI) must be applied to online/digital issues and disputes.

Law stated - 19 August 2026

ADR

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

The Federal Public Service Economy has created the Belmed platform that facilitates alternative dispute resolution through the internet by bringing both parties together in a platform and also providing access to partners to act as mediator. Its scope is not limited to online/digital disputes. The parties can also engage qualified mediators or mediation institutions such as CEPANI. Various sectors, organisations and professional associations have also set up ADR bodies that can be involved in dispute resolution.

Law stated - 19 August 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

The world of digital technologies is growing exponentially and poses new challenges to existing legal frameworks due to the novel issues it creates. The European legislator has boosted efforts in recent months to cope with these rapid evolutions, proposing and introducing laws that will significantly impact digital transformation and online businesses. The AI Regulation, which entered into force on 1 August 2024 with a phased implementation schedule (as since amended by the Digital Omnibus on AI of June 2026, which postponed the application of the high-risk requirements to 2 December 2027 and 2 August 2028), is one of the first comprehensive global laws on artificial intelligence (AI), potentially clearing the way forward for other jurisdictions to regulate this technology as was the case for privacy with the General Data Protection Regulation. Although the AI Regulation mainly governs 'high-risk' AI systems, it puts forward important principles (eg, the quality of data sets and transparency obligations) that could be applied similarly to other AI products. Certain jurisdictions may become inspired by these rules and also extend them voluntarily to other systems. The new Product Liability Directive (EU) 2024/2853, which entered into force on 8 December 2024 and must be transposed by the Member States by 9 December 2026, tackles further issues with respect to the liability rooted in AI and Internet of Things systems by extending strict product liability to software (including AI systems) and easing the burden of proof for injured persons. The separate proposal for an AI Liability Directive was withdrawn by the European Commission in February 2025.

Cybercrime continues to be a challenge for many countries, including Belgium. The revised NIS Directive (NIS 2), with an expanded scope of application, may further boost cybersecurity efforts from a legal standpoint. The proposed ePrivacy Regulation, which was intended to provide more clarity regarding specific issues that may arise concerning privacy in connection with online interactions and electronic communications, was formally withdrawn by the European Commission in February 2025, after negotiations had stalled for almost eight years. Instead, the Commission's 'Digital Omnibus' package of 19 November 2025 proposes to modernise and streamline the existing framework by, among other things, integrating the cookie and terminal-equipment rules of the ePrivacy Directive into the General Data Protection Regulation and introducing targeted simplifications of the GDPR, the Data Act and the NIS2 Directive. These proposals are still being negotiated by the European Parliament and the Council; only the AI-related part of the Digital Omnibus has been adopted to date.

The Markets in Crypto-Assets Regulation (MiCA), the first comprehensive crypto regulation in Europe, has been fully applicable since 30 December 2024, replacing the previous national rules on crypto exchanges and wallets. The transitional period during which existing crypto-asset service providers could continue to operate under national law ended on 1 July 2026, so that all crypto-asset service providers active in Belgium now require a MiCA authorisation. The Belgian Law of 11 December 2025 divides the authorisation and supervisory powers under MiCA between the FSMA and the National Bank of Belgium, and the FSMA took its first enforcement actions against unauthorised providers in July 2026. Crypto-assets that qualify as financial instruments remain subject to the existing financial legislation.

Additionally, the Digital Services Act and the Digital Markets Act have come into force, regulating online intermediaries and platforms, and addressing 'gatekeepers' in digital markets. While the full impact of these regulations remains to be seen, they are expected to significantly affect tech giants by promoting competition in the digital market. It will be intriguing to observe how effective these new rules are and whether they can transform the sector.

The introduction of the above legislation in a way that also meets business interests and innovation can potentially make Europe indeed fit for the digital age – the European Commission's goal.

Law stated - 19 August 2026



Steven De Schrijver

sds@allegiance.law

[Read more from this firm on Lexology](#)

Chile

Claudio Magliona, Carlos Araya

Magliona Abogados

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The Chilean government takes a proactive and positive approach to internet-related issues, demonstrating a strong commitment to fostering the use and growth of new technologies. The government has implemented a dedicated public policy, known as its digital strategy, aimed at enhancing technology adoption as a key driver of Chile's progress. This digital strategy seeks to increase technology use across companies, government entities, and universities, while also establishing an appropriate legal framework to support these objectives.

Law stated - 26 August 2025

Legislation

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

There isn't a single, comprehensive piece of legislation governing business on the internet in Chile. However, specific laws have been enacted to address various internet-related issues, including e-signatures, data protection, computer crime, internet as a public service, fintech law, intellectual property and internet neutrality, as well as consumer protection. Additionally, general provisions from broader Chilean laws, such as the Constitution, Civil Code and Commerce Code, also apply to internet business activities.

Law stated - 26 August 2025

Regulatory bodies

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

There are no specific regulatory bodies directly responsible for the regulation of e-commerce in Chile. However, various agencies oversee specific areas related to e-commerce. The consumer protection agency, SERNAC, ensures compliance with protective provisions in B2C electronic agreements.

The Government Agency of Telecommunications (SUBTEL) classifies internet services as complementary telecommunications services, which do not require a licence or permit to provide internet access. Nonetheless, SUBTEL supervises internet service providers (ISPs) to ensure their compliance with the Telecommunications Act, although ISPs are free to set their tariffs and charges.

Data protection in Chile is currently governed by Law No. 19,628 on Protection of Private Life. This law regulates both automatic and non-automatic processing of personal data by government or private entities in data registries. Currently, there is no dedicated data protection agency or authority. However, this is set to change with the enactment of Law No. 21.719, published in December 2024, which modernises the Chilean data protection framework and brings it closer to international standards such as the EU GDPR. Once fully in force (expected by December 2026), the law will establish an independent Data Protection Authority (*Agencia de Protección de Datos Personales*), endowed with broad supervisory powers including enforcement, investigations, and the ability to impose administrative sanctions.

Lastly, Chile has a net neutrality law establishing the principle that ISPs cannot discriminate against content. The law also sets minimum conditions that ISPs must fulfil in providing internet access services, including mandatory website disclosure of service levels, such as speed, service-level agreements, network management actions, traffic control, and both local and international connection quality standards. SUBTEL supervises these requirements.

Law stated - 26 August 2025

Jurisdiction

- 4 | 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?

Chile does not have a specific statutory "targeting" or "effects" test for online transactions. Normally, a company with only an online presence in Chile would not be subject to Chilean law or the jurisdiction of Chilean courts, unless the parties agree to submit the dispute to Chilean law or to the Chilean courts, which is enforceable in Chile. However, it is important to note that certain acts and contracts, as a matter of Chilean public policy, will be subject to Chilean law regardless of the parties' agreement (eg, when goods are located in Chile, local law applies).

Law stated - 26 August 2025

Establishing a business

- 5 | 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?

Chilean law does not establish a separate incorporation regime for digital businesses. If a digital business company wishes to establish a physical presence in Chile, it must comply with all regulatory and procedural requirements applicable to brick-and-mortar businesses, including incorporation under the applicable corporate form, registration with the Chilean

Internal Revenue Service (SII), tax commencement of activities, accounting and invoicing compliance, and, where applicable, a municipal business licence and sector-specific permits. The principal differences arise not at the incorporation stage, but in the operation and sale of digital content or services.

Law stated - 26 August 2025

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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, Chilean law allows for the formation and execution of legal contracts digitally. Law No. 19.799 on Electronic Documents, Electronic Signatures and Certification Services (the E-Signature Act) expressly recognises the legal validity and enforceability of electronic contracts and signatures, provided the parties consent to use electronic means. Contracts are formed in the same way as traditional ones—through offer and acceptance—expressed electronically. Advanced Electronic Signatures (AEF) have the same legal effect as handwritten signatures in most cases. However, exceptions apply: certain contracts, such as family law agreements, wills, and those requiring public deed (eg, real estate transfers), must be executed in a formal manner and are not valid if concluded entirely electronically.

Law stated - 26 August 2025

Applicable laws

- 7 | 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?

Under Chilean law, parties are generally free to choose the governing law, language, and forum in digital contracts—particularly in B2B transactions. However, in B2C contracts, consumer protection rules under Law No. 19.496 prevail. These include mandatory jurisdiction in the consumer's domicile (Article 50), and any clause that waives consumer rights—such as applying foreign law or foreign forums—may be deemed abusive and unenforceable. Therefore, while freedom of contract applies in B2B settings, B2C contracts are subject to overriding local protections that limit party autonomy in these matters.

Law stated - 26 August 2025

Electronic signatures

- 8 | 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?

The E-Signature Act recognises two types of electronic signatures: the standard electronic signature and the advanced electronic signature. A standard electronic signature is defined as any 'sound, symbol, or electronic process that enables the recipient of an electronic document to at least formally identify its author'. In contrast, an advanced electronic signature is defined as one 'created using means exclusively controlled by the holder, such that it is linked to the holder and the data it references, allowing for the detection of any alterations, verification of the holder's identity, and prevention of repudiation of its integrity and authorship'. This advanced signature must be certified by a registered third party.

Law stated - 26 August 2025

Breach

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

The remedies available for the breach of electronic contracts are the same as for non-electronic contracts. This equality is expressly manifested in the law on electronic signatures by recognising the principle of equivalence of media. This principle imposes the recognition of the same effects of the act or contract consisting of electronic means as it would have if it were made by other traditional means. Its application is no more than the materialisation of the principle of equality before the law and its objective is non-discrimination in relation to the media, in terms of legal effects, validity or binding force.

Law stated - 26 August 2025

FINANCIAL SERVICES

Regulation

- 10 | 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?

General rules apply to the advertising and sale of financial services products to consumers or businesses via the internet, as there is no specific regulation governing these activities. Consequently, activities such as third-party asset management, lending, money brokerage, insurance services, and the public offering of securities are restricted to legally authorised entities, and any advertising must comply with specific regulations. The Consumer Protection Act includes several provisions regarding the requirements for financial services contracts. Additionally, the Financial Market Commission (CMF) has issued guidelines covering various aspects, including fair treatment of customers by financial institutions, proper management of conflicts of interest, protection of customer information, transparency in the marketing and advertising of financial products, and diligent handling of complaints and filings.

Law stated - 26 August 2025

Electronic money and digital assets

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

Yes, Chile regulates electronic money, digital assets, and cryptocurrencies under the 2023 Fintech Law (Law No. 21.521). The Central Bank oversees the issuance of electronic money and fiat-backed stablecoins, while the CMF regulates crypto-asset service providers, who must register and comply with AML, governance, and consumer protection rules. B2C and B2B offerings are both subject to oversight. Tax obligations apply, and an Open Finance framework is being phased in. Although the Central Bank is exploring a retail Central Bank Digital Currency, no official issuance has occurred yet.

Law stated - 26 August 2025

Digital and crypto wallets

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

Yes, Chile regulates the provision of crypto wallets and digital value storage under the Fintech Law (Law No. 21.521). Custodial wallet providers must register with the CMF and comply with governance, cybersecurity, and AML/KYC requirements. Wallets storing fiat-backed digital money are additionally subject to Central Bank oversight. Non-custodial wallets face fewer regulatory obligations but may still trigger compliance duties if linked to financial services or exchange operations. Tax reporting and consumer protection rules also apply.

Law stated - 26 August 2025

Electronic payment systems

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

Electronic payment systems in Chile are regulated under the Fintech Law (Law No. 21.521) and supervised by both the CMF and the Central Bank of Chile (BCCh). The CMF oversees registration and compliance for non-bank payment service providers (eg, digital wallets, payment initiators), including AML/KYC, operational risk, and cybersecurity requirements.

The BCCh, under its Organic Law, plays a key role in safeguarding the integrity and interoperability of the national payment system. It regulates and authorises low-value clearinghouses and is leading the development of 'Bre B', a new real-time retail payment system that will enable interoperable access to banks, fintechs, and wallets. Bre B is expected to launch in late 2025.

Additionally, the BCCh and CMF are jointly implementing Chile's Open Finance framework, which requires banks and financial institutions to share customer data with licensed third parties via secure APIs—subject to the consumer's explicit consent. Several draft regulations related to clearinghouses and infrastructure standards are currently under public consultation as part of this implementation.

Law stated - 26 August 2025

Online identity

- 14** | 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?

Yes, Chile allows the use of third parties to fulfill KYC and AML obligations, but the regulated entity remains fully responsible for compliance. Under updated rules from the Financial Analysis Unit (UAF), including Circular No. 62, outsourcing is permitted if based on a documented risk assessment and subject to strict oversight. Contracts must clearly define responsibilities, and regulated entities must monitor, audit, and report suspicious activities, regardless of whether services are outsourced. These rules apply across financial, fintech, and crypto sectors.

Law stated - 26 August 2025

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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 Network Information Centre Chile (NIC) is the entity responsible for registering .cl top-level domain names, which identify Chile on the internet. In this role, NIC is accountable to both the local and global internet communities for the secure and efficient operation of these domains, enabling individuals, businesses and institutions to establish their online identity under the .cl domain. NIC's authorisation originates from the Internet Assigned Numbers Authority.

The process for registering a domain name must be completed exclusively through electronic means, either via email or the NIC website. Upon application, NIC will automatically send a statement confirming that the applicant complies with NIC's terms and conditions. A registration fee of US\$40 is charged by NIC. After payment, the application is published on the NIC website for 30 days, allowing third parties to acknowledge or challenge the applicant's right to the domain name. If the domain name goes unchallenged during this period, the applicant will receive notification of the successful registration. If

the domain name is challenged or if multiple applications for the same domain name are submitted, the dispute will be resolved by an arbitration panel.

According to NIC rules, any individual currently domiciled in Chile, as well as legal entities, whether public or private, that are incorporated in Chile or are properly authorised to operate in Chile, may request the registration of a domain name. Foreign applicants can apply for a .cl domain name through a third party domiciled in Chile, with the application explicitly stating that the third party is acting as an agent.

Law stated - 26 August 2025

IP ownership

- 16** | 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?

Domain names or URLs may be subject to trademark or copyright protection in Chile, provided they meet the relevant legal requirements. Chilean law protects trademarks by recognising a property right over expressions and distinctive signs. However, this protection is limited to the products and services covered by the corresponding registration. Therefore, the owner of a trademark does not automatically have the right to a domain name on the internet simply by virtue of holding a trademark registration.

A challenge to an existing domain name will only be effective if it infringes the scope of the trademark's protection. There are two primary ways a trademark may interfere with a domain name:

- as the basis for a preferential interest in an early revocation request of a domain name within the 30-day period following the publication of the application; and
- as a factor in filing a late revocation request of a domain name after the 30-day publication period.

In relation to copyright, it is more challenging to establish a conflict with a domain name, as it is difficult for a word or phrase to meet the legal requirements necessary to be considered a work protected by copyright.

Law stated - 26 August 2025

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

Online advertising in Chile is governed primarily by the Consumer Protection Law (Law No. 19.496), which prohibits false, misleading or insufficient advertising and applies across all media, including websites, apps, marketplaces, social networks and influencer marketing.

SERNAC has issued interpretative guidance on native advertising and influencers, requiring that commercial content be clearly identifiable as advertising where a commercial link exists between the advertiser and the publisher or influencer. Additional restrictions may apply depending on the product or audience, including rules on food advertising to children under Law No. 20,606, tobacco, alcohol, medicines, financial products, gambling, intellectual property, unfair competition and personal data processing. CONAR's Chilean Code of Advertising Ethics also provides self-regulatory standards, including rules on digital advertising, influencers and AI-generated advertising content.

Law stated - 26 August 2025

Targeted advertising and online behavioural advertising

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

Chile does not have a specific statute governing targeted advertising or online behavioural advertising as such. However, these practices are regulated through general consumer protection, advertising and personal data rules. Where targeting involves the collection or processing of personal data, online identifiers, browsing behaviour, profiles or data shared with advertising networks, the provider must comply with Law No. 19,628 on Protection of Private Life, including notice and a valid legal basis, typically consent, unless another legal authorisation applies. Law No. 19,496 on Consumer Protection also requires advertising to be truthful, clear and not misleading, and SERNAC guidance requires commercial content, including influencer or native advertising, to be identifiable as advertising. From December 2026, Law No. 21,719 will materially strengthen the data protection framework, including transparency, lawful bases, data subject rights and rules relevant to profiling and automated processing.

Law stated - 26 August 2025

Misleading advertising

19 | Are there rules against misleading online advertising?

Yes. Misleading online advertising is prohibited in Chile under Law No. 19,496 on Consumer Protection, which applies to advertising disseminated through any medium, including websites, apps, marketplaces, social networks, search advertising and influencer or native advertising. Under article 28, a supplier infringes the law where, through advertising, it induces or may induce consumers to error regarding matters such as the characteristics, composition, origin, suitability, price, payment terms, credit cost, warranty conditions or environmental qualities of a product or service. Article 28 A also prohibits advertising that creates confusion among consumers regarding the identity of companies, activities, products, names, brands or other distinctive signs of competitors. Advertising claims should be truthful, clear, verifiable and substantiated. SERNAC may enforce consumer advertising rules, and affected consumers may seek statutory remedies before competent courts.

Law stated - 26 August 2025

Restrictions

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

Yes. Chilean law restricts or prohibits the online advertising of certain products and services, although the restrictions usually arise from the nature of the product or service rather than from its digital format. Tobacco advertising is heavily restricted under Law No. 19,419. Food and beverages classified as high in calories, sugar, sodium or saturated fat are subject to advertising restrictions under Law No. 20,606, particularly where advertising is directed at children under 14. Alcoholic beverages are subject to specific advertising limitations under Law No. 21,363. Financial products, securities, insurance, payment services and other regulated financial services may only be promoted where the underlying activity is legally authorised and the advertising complies with Financial Market Commission and consumer protection rules. Medicines, health products, gambling, betting and other regulated or unlawful services may also face specific prohibitions, licensing requirements or content restrictions.

Law stated - 26 August 2025

Direct email marketing

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

Direct marketing by email, SMS, telephone or similar channels is regulated mainly by Law No. 19,496 on Consumer Protection and by Chilean personal data protection rules. Article 28 B of Law No. 19,496 requires promotional or advertising emails to state the subject matter, identify the sender and include a valid address through which the recipient may request suspension of further messages; once the recipient opts out, further promotional emails are prohibited. The same provision allows consumers receiving promotional communications by postal mail, fax, telephone calls or messaging services to request suspension. The Consumer Protection Agency (has implemented a tool called Do Not Disturb, which allows Chilean consumers to request the removal of their contact information from company lists to stop receiving unwanted advertising, such as emails, phone calls and text messages. Through this tool, consumers can exercise their right, as recipients of emails, phone calls or text messaging services, to request the suspension of promotional or advertising communications they do not wish to receive (Consumer Protection Act, article 28 B).

Law stated - 26 August 2025

ONLINE PUBLISHING

Hosting liability

I

- 22** | 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?

Chile does not have a general statutory safe-harbour regime for all third-party online content. The most developed rules concern copyright. Law No. 17,336, as amended by Law No. 20,435, limits liability for qualifying internet service providers, including transmission, caching, hosting and information-location services, where they meet the statutory conditions. For hosting providers, this generally requires lack of effective knowledge of infringing content, absence of direct financial benefit where the provider has the right and ability to control the activity, public designation of a representative to receive notices, and removal or disabling of access following a court order or other applicable legal notice. Providers should minimise liability through clear terms of use, complaint and takedown procedures, repeat-infringer policies, records of notices and actions taken, IP and content-moderation policies, and cooperation with lawful authority requests.

Law stated - 26 August 2025

Content liability

- 23** | 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 for inaccurate information that it publishes itself under the ordinary rules applicable to the nature of the content and resulting harm. Potential bases include contractual liability, tort liability under the Civil Code, consumer protection liability under Law No. 19,496 where information or advertising is false, misleading or insufficient, unfair competition, defamation, intellectual property infringement, data protection breaches and sector-specific rules, such as those applicable to financial, health or regulated professional content. Liability will depend on factors such as authorship, control, negligence, reliance, damage and applicable statutory duties. The provider may reduce risk through clear terms of use, editorial review, source attribution, correction procedures, date stamps, disclaimers and notices distinguishing general information from advice. However, notices cannot exclude mandatory consumer, advertising, regulatory or tort liability where the legal requirements for liability are met.

Law stated - 26 August 2025

Shutdown and takedown

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

As a general rule, an internet service provider or telecommunications provider should not unilaterally shut down a webpage merely because a third party alleges that it contains

defamatory material. Chile does not have a general statutory notice-and-takedown regime for defamation equivalent to the copyright safe-harbour rules under Law No. 17,336, where takedown is linked to statutory procedures and, in relevant cases, court orders. Whether content is defamatory, injures honour or privacy, or is otherwise unlawful is normally a matter for the courts. An affected person may seek civil or criminal remedies, or file a constitutional protection action where fundamental rights are affected, and request removal, blocking or other interim measures. Providers may act under their contractual terms for clearly unlawful or policy-violating content, but should minimise risk by requiring substantiated notices, preserving evidence and acting consistently with due process, neutrality and freedom of expression.

Law stated - 26 August 2025

INTELLECTUAL PROPERTY

Data and databases

25 | Are data and databases protected by IP rights?

Data as such is not protected by copyright in Chile. However, databases may be protected where, by reason of the selection or arrangement of their contents, they constitute an intellectual creation. Article 3 No. 17 of Law No. 17,336 on Intellectual Property expressly protects compilations of data or other materials, in machine-readable or other form, where their selection or arrangement is original, but clarifies that this protection does not extend to the underlying data or materials themselves. Chile does not recognise a separate *sui generis* database right equivalent to the European Union database right. Accordingly, non-original datasets or raw data will generally need to be protected, where possible, through contracts, confidentiality obligations, trade secret rules, technological controls, personal data protection law where personal data is involved, and unfair competition rules in cases of improper appropriation or use.

Law stated - 26 August 2025

Third-party links and content

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

As a general rule, Chilean law does not require a website, digital platform or online content provider to obtain permission merely to link to a third-party website or platform. However, linking may create liability where it forms part of infringing or unlawful conduct, such as facilitating copyright infringement, misusing trademarks, creating consumer confusion, engaging in unfair competition, bypassing access restrictions, violating privacy or personal data rules, or directing users to unlawful content. Law No. 17,336 on Intellectual Property includes liability limitations for qualifying internet service providers, including information-location, linking or reference services, subject to statutory conditions; however, these safe harbours are specific to copyright and do not provide a general immunity for

all third-party content. Platforms should use clear terms, avoid misleading presentation of links, respect takedown or court orders, and act promptly when notified of unlawful content.

Law stated - 26 August 2025

- 27** | 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?

A website, digital platform or online content provider should not assume that third-party content obtained through automated scraping or other means may be used without permission. Chile has no general statute prohibiting web scraping as such, but the legality of scraping and reuse depends on the nature of the content, the method of access and the intended use. Reuse of protected works may infringe Law No. 17,336 on Intellectual Property unless authorised, in the public domain, or covered by a statutory exception. Databases may also be protected where their selection or arrangement is original. Scraping may additionally raise issues under website terms, confidentiality or trade secret rules, unfair competition, computer crime law, consumer law, cybersecurity rules and personal data protection law. In regulated sectors, such as finance, access to customer data is increasingly channelled through the Open Finance framework under Law No. 21,521.

Law stated - 26 August 2025

Metaverse and online platforms

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

Chile has no specific intellectual property regime for the metaverse or virtual environments. General IP rules therefore apply regardless of the medium. Copyright under Law No. 17,336 may protect original works used or created in a metaverse, including software, audiovisual works, music, visual art, avatars or virtual objects, but ordinary issues of authorship, ownership, licensing, platform terms, evidence of infringement and cross-border enforcement may be more complex. Databases are protected only where the selection or arrangement of their contents constitutes an intellectual creation; Chile does not recognise a separate sui generis database right. Trademarks under Law No. 19,039 may also be enforced in virtual environments, but difficulties may arise in proving use in commerce, likelihood of confusion, territorial connection with Chile, classification of virtual goods or services, and the identity of infringers.

Law stated - 26 August 2025

Exhaustion of rights and first-sale doctrine

- 29** | 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?

Chile recognises exhaustion of rights in copyright. Under article 18 of Law No. 17,336 on Intellectual Property, the first sale or other transfer of ownership of the original or a copy, whether in Chile or abroad, exhausts the author's distribution right nationally and internationally in respect of that copy. However, Chilean law does not expressly regulate how exhaustion applies to digital products, downloads, SaaS, NFTs or metaverse assets, and there is limited judicial guidance on this point. The doctrine should be easier to apply where there is a true transfer of ownership of a specific copy, and more difficult where the transaction is structured as a licence, access right or service. Placing a digital product on a foreign platform or metaverse should not automatically exhaust Chilean rights unless the legal requirements for a qualifying transfer are met.

Law stated - 26 August 2025

Administrative enforcement

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

Chilean authorities may participate in IP enforcement, but dawn raids, seizures and freezing-style injunctions generally require judicial authorisation rather than being imposed administratively by IP authorities. Border measures are available under Law No. 19,912, allowing the suspension of customs clearance of goods suspected of infringing trademarks or copyrights, usually through a court order and with the involvement of the National Customs Service. In criminal IP cases, prosecutors may request investigative measures, and police authorities may execute searches, seizures or raids under the Criminal Procedure Code, subject to the applicable judicial approvals. In civil proceedings, courts may order preliminary or interim measures, including suspension of infringing acts, seizure or retention of infringing goods, materials or proceeds, and other measures to preserve evidence or prevent further infringement. The INAPI does not itself conduct raids or issue freezing injunctions.

Law stated - 26 August 2025

Civil remedies

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

IP owners in Chile may seek civil remedies under the applicable IP statutes, principally Law No. 17,336 on Intellectual Property and Law No. 19,039 on Industrial Property. Available remedies include cessation of the infringing conduct, damages, destruction or removal of infringing goods, publication of the judgment, seizure or retention of infringing goods or materials, and other measures aimed at preventing continuation of the infringement or preserving evidence. Chilean law does not use the common-law terminology of “search orders” or “freezing injunctions”, but courts may grant prejudicial or precautionary measures where the statutory requirements are met, including urgency, plausibility of the

right and risk of harm or dissipation. Such measures may include seizure, retention of assets, appointment of receivers, prohibition of advertising or sale, and suspension of infringing acts.

Law stated - 26 August 2025

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

- 32** | 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?

Under Law No. 19,628 on Protection of Private Life, personal data is any information concerning identified or identifiable natural persons. The law also recognises sensitive personal data, meaning personal data referring to a person's physical or moral characteristics or to facts or circumstances of private life or intimacy, such as personal habits, racial origin, ideologies, political opinions, religious beliefs, physical or mental health conditions, and sex life. Sensitive data may only be processed where authorised by law, with the data subject's consent, or where necessary for the determination or granting of health benefits. Law No. 21,719, which will enter into force on 1 December 2026, modernises this framework and strengthens rules on sensitive data, children's data, lawful bases, data subject rights and supervisory enforcement.

Law stated - 26 August 2025

Registration and appointment of data protection officer

- 33** | 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?

Under current Chilean law, private parties are not generally required to register with a data protection regulator before processing personal data. Law No. 19,628 requires databases managed by public bodies to be registered with the Civil Registry and Identification Service, including information on their legal basis, purpose, type of data and data subjects covered. Chilean law also does not currently require private controllers or processors to appoint a data protection officer. Law No. 21,719, which will enter into force on 1 December 2026, will substantially modernise the regime by creating the Personal Data Protection Agency and strengthening accountability, governance and enforcement obligations. However, it does not establish a general prior-registration requirement for all private databases. Organisations may nevertheless need to designate responsible internal roles or compliance functions as a matter of good governance, sector regulation or risk management.

Law stated - 26 August 2025

Extraterritorial issues

- 34** | 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?

Under current Law No. 19,628, Chilean data protection law does not contain a detailed extraterritoriality rule comparable to the GDPR, nor does it generally require a foreign controller or processor to appoint a representative in Chile solely to process personal data. However, Chilean rules may be relevant where the processing has a sufficient connection with Chile, such as where data is collected, processed, communicated or used in Chile, or where Chilean residents' rights are affected. Data subjects are protected regardless of nationality. Law No. 21,719, which will enter into force on 1 December 2026, will materially expand and clarify the territorial scope of Chilean data protection law, including its application to certain foreign controllers or processors whose activities target persons located in Chile or monitor their behaviour, and will create a specialised Personal Data Protection Agency.

Law stated - 26 August 2025

Bases for processing

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

Currently, under Law No. 19,628, the principal basis for processing personal data is the data subject's authorisation, unless a statutory exception applies. Processing must also comply with purpose limitation, legality, proportionality and information duties. Commonly relied-upon exceptions include data obtained from publicly accessible sources, where the statutory conditions are met, processing by private entities for their exclusive internal use, and specific legal authorisations for particular sectors or purposes. Cross-border transfers are not regulated through a detailed adequacy or transfer-mechanism system under the current law, but they are generally treated as processing or communication of personal data and therefore require a valid basis, appropriate notice and compliance with the original purpose. Law No. 21,719, effective from 1 December 2026, will introduce a broader lawful-basis framework and more detailed rules for international data transfers, including safeguards and regulatory oversight.

Law stated - 26 August 2025

Data export and data sovereignty

- 36** | 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?

Current Law No. 19,628 does not contain a detailed regime for international transfers of personal data, nor does Chile impose a general data localisation requirement obliging personal data, servers or databases to remain in Chile. However, exporting or transferring personal data abroad is generally treated as a form of processing or communication of personal data and must therefore have a valid legal basis, comply with the purpose for which the data was collected, and satisfy applicable information and consent requirements. Sector-specific rules may impose additional confidentiality, security, outsourcing or regulatory-access obligations, particularly in financial, health, telecom, public-sector and critical-infrastructure contexts. Law No. 21,719, effective from 1 December 2026, will introduce a more detailed framework for international data transfers, including adequacy-type mechanisms, safeguards and regulatory oversight by the new Personal Data Protection Agency.

Law stated - 26 August 2025

Sale of data to third parties

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

Yes, personal data may be sold or transferred to third parties in Chile, but only where the transfer complies with applicable data protection rules. Under current Law No. 19,628, the sale or transfer of personal data is treated as processing or communication of data and generally requires the data subject's authorisation, unless a statutory exception applies. The controller must inform the data subject of the purpose of the processing and the possible communication of the data, and the transfer must remain consistent with the purpose for which the data was collected. Particular care is required where data concerns users of an online service or platform, because additional consumer, confidentiality, cybersecurity and contractual obligations may apply. Law No. 21,719, effective from 1 December 2026, will introduce a more developed framework for lawful bases, transparency, data subject rights, international transfers and regulatory enforcement.

Law stated - 26 August 2025

Consumer redress

38 | 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?

According to the Law No. 19,628, individuals have rights to request information about the processing of their personal data, including its origin, purpose, recipients and persons or entities to whom the data is regularly disclosed. They may also request correction of inaccurate, outdated, incomplete or misleading data, deletion or cancellation where storage lacks legal basis or the data has expired, blocking in certain cases, and opposition to the use of their data for advertising, market research or opinion surveys. These rights are

not limited to Chilean citizens and may be exercised by any data subject whose personal data is processed under Chilean law. Breaches may give rise to judicial claims, fines and compensation for material and moral damages caused by wilful misconduct or negligence. Law No. 21,719, effective from 1 December 2026, will expand and modernise these rights and enforcement mechanisms.

Law stated - 26 August 2025

Non-personal data

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

No, Chile does not currently have a general statute regulating the use, access, sharing or portability of non-personal data as a standalone category. Data protection law applies to personal data concerning identified or identifiable natural persons, not to genuinely anonymous or non-personal data. However, non-personal data may still be subject to legal restrictions under other regimes, including contractual terms, confidentiality obligations, trade secret protection, cybersecurity duties, intellectual property rights in original databases or compilations, unfair competition rules, sector-specific regulation and public-sector information rules. In practice, the key issue is whether the data is truly non-personal. Pseudonymised, aggregated or anonymised datasets may still fall within personal data rules if individuals can reasonably be re-identified. Law No. 21,719, effective from 1 December 2026, will strengthen the distinction between personal data, anonymised data and other forms of data processing.

Law stated - 26 August 2025

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

Chilean law generally recognises the validity of electronic documents and electronic signatures under Law No. 19,799, so many contracts and business records may be created, signed and retained electronically. However, this does not mean that all paper documents may safely be destroyed after digitisation. Original paper form or additional formalities may still be required where the law demands a solemnity incompatible with an electronic document, the personal attendance of a party, a public deed, notarial or registry formalities, or specific original records for evidentiary, tax, labour, corporate, regulatory or sector-specific purposes. Examples may include certain real estate, mortgage, succession, family law, negotiable instrument, notarial and public registry matters. Businesses should therefore assess retention requirements by document type before relying solely on digital copies, even where electronic records are generally admissible.

Law stated - 26 August 2025

Retention

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

Chilean law does not establish a single minimum or maximum retention period applicable to all business documents. Retention periods vary depending on the type of record, the applicable limitation period and the relevant regulatory framework. As a general reference, tax and accounting records, including electronic tax documents, must usually be retained for six years, subject to longer retention where the records remain relevant to tax periods that are not yet time-barred. Labour documentation relating to current and former employees must generally be retained for at least five years after termination of the employment relationship. Consumer, corporate, financial, health, telecommunications, cybersecurity, public procurement and sector-specific rules may impose additional or longer retention duties. Personal data should not be retained longer than necessary for the lawful purpose of processing, particularly under the strengthened framework introduced by Law No. 21,719.

Law stated - 26 August 2025

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

Chile does not impose a single cybersecurity standard on all companies. Obligations depend on the sector, the type of data processed and whether the entity is classified as an essential service provider or operator of vital importance under Law No. 21,663, the Cybersecurity Framework Law. That law creates the National Cybersecurity Agency (ANCI), the National Computer Security Incident Response Team (CSIRT) and a risk-based framework requiring covered entities to implement permanent cybersecurity duties, manage risks, maintain information security systems, report significant cybersecurity incidents and comply with technical standards issued by the authority. Sector-specific rules may impose additional requirements, particularly for banks, financial institutions, payment systems, telecommunications, health, utilities and public-sector contractors. Commonly used standards include ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework and, for payment card environments, PCI DSS, although their mandatory status depends on the applicable regulation or contract.

Law stated - 26 August 2025

Data breach notification

I

- 43** | 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?

No, Chile does not currently have a general personal data breach notification obligation applicable to all digital businesses under Law No. 19,628. However, Law No. 21,663, the Cybersecurity Framework Law, requires entities within its scope, including essential service providers and operators of vital importance, to report significant cybersecurity incidents to the National CSIRT and comply with the reporting procedures established by ANCI and related regulations. Sector-specific notification duties may also apply, particularly in financial services, payment systems, telecommunications, health, public-sector contracting and regulated infrastructure. Affected individuals must generally be notified where required by sector-specific law, court or regulator order, contractual duties, consumer protection considerations or risk-management best practice. Law No. 21,719, which enters into force on 1 December 2026, will introduce a general personal data breach notification framework involving the new Personal Data Protection Agency and, in certain cases, affected data subjects.

Law stated - 26 August 2025

Government interception

- 44** | 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?

Yes, Chilean authorities may lawfully access data under specific legal frameworks. In criminal investigations, prosecutors may request, and courts may authorise, access to stored data, searches, seizures or interception of communications under the Criminal Procedure Code and sector-specific rules, particularly where privacy or secrecy of communications is affected. Telecommunications providers, internet service providers and digital platforms may therefore be required to preserve or disclose information when ordered by a competent authority. Financial institutions and regulated entities must also provide information to regulators such as the Financial Market Commission and to the Financial Analysis Unit under financial supervision and AML rules. Essential service providers and operators of vital importance must report significant cybersecurity incidents under Law No. 21,663. From December 2026, the Personal Data Protection Agency will also have supervisory powers under Law No. 21,719.

Law stated - 26 August 2025

GAMING

Legality and regulation

- 45** | 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?

Operating an online betting or gaming business from Chile is not currently permitted under a general online gambling licence. Chilean law follows the principle that gambling is unlawful unless expressly authorised by statute. Existing authorisations cover limited activities, including licensed land-based casinos under Law No. 19,995, state lottery operators, horse-racing betting and specific legally authorised games of chance. Online betting and casino platforms are not yet subject to a fully operative licensing regime, and the Supreme Court has held that unauthorised online gambling services are illegal unless expressly authorised. A bill to regulate online betting platforms has advanced in Congress, including approval in general by the Senate in August 2025, but until enacted and implemented it does not provide regulatory consent. If a future regime is adopted, age verification, identity checks, responsible-gaming controls, tax, AML and advertising restrictions are expected to apply.

Law stated - 26 August 2025

Cross-border gaming

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

Advertising or providing access in Chile to an online betting or gaming business located abroad, or in a metaverse environment, is legally risky unless the activity is expressly authorised under Chilean law. Chile follows the principle that gambling is unlawful unless permitted by statute, and current authorisations are limited to specific operators and activities, such as licensed land-based casinos, state lottery operators, horse-racing betting and other legally authorised games. Foreign licensing does not by itself authorise offering, advertising or facilitating access to gambling services for users in Chile. The Supreme Court has treated unauthorised online gambling as illegal and has ordered blocking measures against unlawful sites. A bill to regulate online betting has advanced in Congress, but until enacted and implemented it does not provide a lawful basis for cross-border or metaverse gambling operations targeting Chile.

Law stated - 26 August 2025

OUTSOURCING

Key legal issues

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

Key legal issues in outsourcing to a provider inside or outside Chile include labour, tax, regulatory, data protection, cybersecurity, intellectual property, confidentiality, service continuity and liability allocation. Where outsourced services are performed in Chile under a subcontracting structure, the principal may be jointly and severally liable for the contractor's labour and social security obligations, unless it exercises statutory information and withholding rights, in which case liability may become subsidiary under the Labour Code.

For technology outsourcing, contracts should address service levels, audit rights, business continuity, incident response, subcontracting, data location and cross-border transfers, ownership of deliverables, licensing of pre-existing IP, confidentiality, exit assistance and transition. In regulated sectors, such as financial services, telecommunications, health, utilities, public-sector services and cybersecurity-critical activities, outsourcing may also require prior regulatory analysis, notifications, minimum contractual clauses or operational risk controls.

Law stated - 26 August 2025

Sector-specific issues

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

No, Chile does not generally prohibit the outsourcing of digital business services, but certain functions are subject to sector-specific regulation and the regulated entity will usually remain responsible for compliance. In financial services, banking, insurance, payment services, securities, fintech and market infrastructure, outsourcing may be subject to Financial Market Commission and Central Bank rules on operational risk, cybersecurity, business continuity, auditability, access to information, subcontracting and regulatory supervision. Telecommunications, health, utilities, public-sector services, gambling and other regulated activities may also impose restrictions, approvals or minimum contractual requirements. Under Law No. 21,663, entities classified as essential service providers or operators of vital importance must ensure cybersecurity and incident-reporting obligations even where functions are outsourced. Separately, labour outsourcing and staffing are regulated under the Labour Code, and personal data processing by vendors must comply with current and forthcoming data protection rules.

Law stated - 26 August 2025

Contractual terms

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

No, Chilean law does not generally prescribe a mandatory set of clauses for all outsourcing contracts. However, specific terms may be required or strongly expected depending on the nature of the services, the industry and whether labour subcontracting, regulated services or personal data processing are involved. In labour subcontracting, the contract should support compliance with the Labour Code rules on contractor responsibility, information rights, withholding rights, social security obligations and workplace health and safety. In regulated sectors, such as banking, financial services, payments, telecommunications, health, utilities and cybersecurity-critical activities, outsourcing contracts may need to address audit rights, regulator access, operational continuity, incident reporting, subcontracting controls and information security. Technology outsourcing contracts should also include clear service levels, data protection and processing terms, confidentiality, IP

ownership and licensing, business continuity, exit assistance, transition, liability allocation and compliance with applicable laws.

Law stated - 26 August 2025

Employee rights

- 50** | 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?

Chilean law does not generally give employees a specific right to consultation or compensation merely because services previously performed internally are outsourced. If outsourcing results in dismissal, affected employees are entitled to the ordinary termination rights and severance payments applicable under the Labour Code, depending on the ground for termination and their individual circumstances. If employees continue to provide services through a contractor, the subcontracting rules in articles 183-A et seq. of the Labour Code may apply. In that case, the contractor remains the employer, but the principal may be jointly and severally liable for the contractor's labour and social security obligations, including statutory severance, unless it exercises statutory information and withholding rights, in which case liability may become subsidiary. Separate and stricter rules apply to temporary staffing services, which are permitted only in limited statutory cases.

Law stated - 26 August 2025

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

No, Chile does not currently have an AI-specific statute in force. However, the development and use of artificial intelligence, machine learning, automated decision-making and profiling are subject to generally applicable rules, including data protection, consumer protection, labour, intellectual property, cybersecurity, anti-discrimination and sector-specific regulation. Where AI involves personal data, Law No. 19,628 applies, and Law No. 21,719, effective from 1 December 2026, will introduce stronger transparency, lawful-basis, data subject rights and automated-processing safeguards. Chile also has a pending AI bill, inspired by a risk-based model, which would classify AI systems by risk and impose obligations on providers, deployers, importers and distributors. There is currently no general mandatory AI impact assessment, but impact assessments are advisable for high-risk uses, especially where profiling, sensitive data, consumer decisions, employment, financial services, health or fundamental rights are involved.

Law stated - 26 August 2025

IP rights

- 52** | 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?

Chile does not currently have specific rules in force governing intellectual property and artificial intelligence or machine learning. Existing IP laws therefore apply. Training datasets may be protected where they contain copyrighted works, confidential information, trade secrets, personal data, or databases whose selection or arrangement is original under Law No. 17,336; however, raw data as such is not generally protected by copyright. The use of third-party works for AI training may require authorisation unless a statutory exception applies. Chile has considered legislative proposals to introduce text and data mining or AI-training exceptions, but these remain subject to legislative debate and should not be treated as settled law. Ownership of AI-generated outputs is also uncertain. Current copyright law is based on human authorship, so purely machine-generated works may face difficulties obtaining protection, while human-assisted works may be protectable if they reflect sufficient human creative contribution.

Law stated - 26 August 2025

Ethics

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

Chile has non-binding public policy guidance on the ethics of artificial intelligence. The National Artificial Intelligence Policy, originally adopted for 2021–2030 and updated in 2024 through Decree No. 12, includes principles and strategic lines on governance, transparency, human rights, inclusion, non-discrimination, safety, sustainability and responsible AI adoption. These policy instruments are not, by themselves, directly enforceable against private parties, but they are relevant for public-sector AI governance and may influence regulatory expectations, procurement standards and future legislation. In addition, ethical AI considerations may become legally relevant through generally applicable rules on personal data protection, consumer protection, labour law, anti-discrimination, cybersecurity, intellectual property and sector-specific regulation. A pending AI bill also proposes a risk-based regulatory model and institutional oversight, but it has not yet entered into force.

Law stated - 26 August 2025

TAXATION

Online sales

|

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

Yes. The sale of digital products and online services may be subject to taxation in Chile, principally through value added tax (VAT) and, depending on the case, income tax or withholding tax rules. Law No. 21,210 introduced a 19 per cent VAT on certain remunerated digital services supplied remotely by non-resident providers to users in Chile, and Law No. 21,713 subsequently extended VAT to all taxed remote services supplied by taxpayers without domicile or residence in Chile. The tax is generally based on consumption or use in Chile. Foreign suppliers may be required to register under the simplified VAT regime, declare and pay VAT, or VAT may be withheld by local payment intermediaries where applicable. B2B transactions may require additional analysis regarding VAT credit, reverse-charge mechanisms, withholding tax and applicable double-tax treaties.

Law stated - 26 August 2025

Server placement

55 | 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?

Placing servers outside the operator's home jurisdiction does not, by itself, determine Chilean tax liability. For a foreign company, placing servers, platform infrastructure or metaverse infrastructure in Chile may create Chilean tax exposure if the infrastructure amounts to a permanent establishment, fixed place of business or other taxable presence, or if the activities generate Chilean-source income. The analysis depends on factors such as permanence, control over the infrastructure, functions performed in Chile, personnel or agents involved, and the applicable tax treaty. Even without a permanent establishment, supplies of digital products or remote services to users in Chile may be subject to 19 per cent VAT under Chile's digital VAT rules, and certain payments to non-residents may trigger withholding tax. Server location is therefore relevant, but not conclusive; the business model, revenue flows and Chilean nexus must be assessed.

Law stated - 26 August 2025

Electronic invoicing

56 | 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?

Yes, Chile has a mandatory e-invoicing regime administered by the Chilean Internal Revenue Service (SII). Taxpayers carrying out taxable activities must generally issue electronic tax documents (DTEs), including electronic invoices, exempt invoices, purchase invoices, debit and credit notes, dispatch guides and export-related documents, in the formats and systems authorised by the SII. Electronic invoices must be digitally signed

by the issuer, use SII-authorised folios and be transmitted to the SII under the applicable technical rules, generally before or in connection with delivery to the recipient, so that their tax validity can be verified. The regime applies broadly across sectors, although specific documents and procedures depend on the transaction. DTEs must also be stored for the legally required retention period, generally six years.

Law stated - 26 August 2025

DISPUTE RESOLUTION

Venues

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

Chile does not have specialist courts dedicated exclusively to online or digital business disputes. Such disputes are generally heard by the ordinary civil courts, commercial arbitration tribunals where validly agreed, or other competent bodies depending on the nature of the claim. Consumer disputes involving digital platforms or e-commerce may be brought before local police courts under Law No. 19,496, with the consumer protection agency (SERNAC) playing an administrative and enforcement role. Industrial property disputes are handled initially by the National Institute of Industrial Property, with appeals to the Industrial Property Court, while copyright disputes are generally heard by ordinary courts. Disputes concerning .cl domain names are resolved through Network Information Centre Chile's arbitration-based system. Sectoral regulators may also intervene in specific matters, including the Financial Market Commission for financial services, Government Agency of Telecommunications for telecommunications, National Cybersecurity Agency for cybersecurity, and, from December 2026, the Personal Data Protection Agency for data protection matters.

Law stated - 26 August 2025

ADR

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

Chile does not have a separate ADR regime exclusively for online or digital disputes, but ordinary ADR mechanisms are available. Arbitration is the most common mechanism in B2B technology, SaaS, outsourcing, software licensing and platform contracts, particularly in higher-value or cross-border transactions, and may be ad hoc or administered by institutions such as the Santiago Arbitration and Mediation Centre (CAM Santiago). Mediation, conciliation and negotiated settlement are also available, although they are less common for complex digital business disputes. In consumer matters, ADR is more limited: consumers may use SERNAC's administrative procedures and collective mechanisms under Law No. 19,496, but contractual clauses that restrict statutory consumer rights, impose abusive terms or unduly limit access to competent courts may be unenforceable.

ADR is therefore common in B2B digital contracts but less developed in mass-market online consumer disputes.

Law stated - 26 August 2025

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

Key digital business trends in Chile include the transition to the new Personal Data Protection Law, Law No. 21,719, which enters into force on 1 December 2026 and creates a specialised supervisory authority; the implementation of the Cybersecurity Framework Law, Law No. 21,663, including National Cybersecurity Agency supervision, incident reporting and the classification of essential service providers and operators of vital importance; and the phased implementation of the Fintech Law and Open Finance framework. Tax compliance for digital marketplaces, payment service providers and remote digital services has also become a priority, particularly following Law No. 21,713 and Chilean Internal Revenue Service Resolution No. 168/2025 on platform and payment-intermediary reporting duties. Other hot topics include the pending AI bill, proposed regulation of online betting platforms, VAT treatment of foreign online gambling services, scrutiny of digital advertising and influencers, and stronger compliance expectations for cross-border cloud, data and platform services.

Law stated - 26 August 2025



Claudio Magliona
Carlos Araya

cmagliona@magliona.cl
caraya@magliona.cl

Magliona Abogados

[Read more from this firm on Lexology](#)

China

[Jan Holthuis](#), [Yongmei Evers Cai](#)

[BUREN](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The Chinese government's general policy is to vigorously support the development of digital technologies while maintaining tight control over the challenges posed by digital content and data flows. Primary laws such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law have been implemented in sequence. Currently, China is further increasing its support for the digital economy by promoting the integration and application of advanced technologies such as 5G, artificial intelligence, big data, and cloud computing, aiming at facilitating the digital transformation of traditional industries and fostering new business models such as online business.

Concurrently, China's regulatory regime has evolved into a highly specialised framework to promote the development of the online platform economy, regulate cross-border data flows, and protect critical data. The Amendment to the Cybersecurity Law explicitly embeds the overall national security view into law while formally encouraging AI technical research and development alongside safety supervision. Comprehensive regulations like the Regulations on Network Data Security Management and national data asset policies further establish a unified framework for data element marketisation separating holding, usage, and operating rights. Moreover, tailored regulatory regimes now cover AI agents, anthropomorphic interactive AI, financial sector AI safety, minor protection online, and personal information cross-border compliance audits.

Law stated - 15 August 2026

Legislation

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

Till now, China has issued extensive laws and regulations related to cyberspace since 2012, forming a relatively comprehensive legal system regulating cybersecurity protection, protection of online individual rights and conduct of business online. The legislation framework is outlined as follows:

Cybersecurity Protection

- Cybersecurity Law (2025 Amendment, effective on 1 January 2026);
- Data Security Law (2021);
- Cybersecurity Review Measures (2021);
-



Regulations on the Security Protection of Computer Information Systems (2011);

- National Security Law (2015);
- Regulations on Network Data Security Management (2024);
- Criminal Law (2024) ; and
- Network Data Security Risk Assessment Measures (2026).

Protection of individual rights

Protection of personal information

- Law on the Protection of Rights and Interests of Consumers (2013);
- Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013);
- Civil Code (2021);
- Cybersecurity Law (2017);
- Personal Information Protection Law (2021);
- Criminal Law (2024);
- Provisions on Certification of Personal Information Outbound Transfer (2026);
- Provisions on Personal Information Protection in Large Online Platforms (Draft for Comment, 2025);
- Provisions on Simplified Personal Information Protection Measures for Small Personal Information Processors (2026); and
- Provisions on Collection and Use of Personal Information by Internet Applications (Draft for Comment, 2026).

Protection of property

- E-Commerce Law (2019, Draft amendment issued for public comment in 2026);
- Civil Code (2021); and
- Anti-Telecom and Online Fraud Law (2022).

Protection of minors

- Regulations on the Online Protection of Children's Personal Information (2019);
- Law on the Protection of Minors (2024);
- Regulations on the Protection of Minors Online (2024);
- Classification Measures for Network Information Potential to Affect Minors' Physical and Mental Health (2026); and

- Interim Measures for the Management of AI Anthropomorphic Interactive Services (2026)

Conduct of business online

- Electronic Signature Law (2019);
- Copyright Law (Amended in 2020);
- Trademark Law (Amended in 2026, effective in 2027);
- Patent Law (Amended in 2020);
- Anti-Monopoly Law (2022);
- Anti-Unfair Competition Law (Amended in 2025);
- Interim Provisions on Anti-Unfair Competition on the Internet (2024);
- Measures for the Supervision and Administration of Online Transactions (Amended in 2025);
- Implementation Rules of Consumer Rights and Interests Protection Law (2024);
- Data Property Rights Registration Work Guidelines (Trial) (2026);
- Provisions on Promoting and Standardizing the Application of Electronic Documents (2026);
- Internet Platform Anti-Monopoly Compliance Guidelines (2026); and
- Internet Platform Price Behavior Rules (2026).

Intermediary liability

- E-Commerce Law (2019 Draft amendment issued for public comment in 2026);
- Regulations on Internet Platform Companies' Submission of Tax-related Information (2025);
- Live Streaming E-commerce Supervision and Management Measures (2026); and
- Rules on the Supervision and Management of Online Transactions Platform (2026)

Telecommunications cybersecurity

- Telecommunications Regulations (2000);
- Regulations on the Security and Protection of Critical Information Infrastructure (2021);
- Administrative Measures on Internet-based Information Services (Amended in 2024);
- Administrative Provisions on Mobile Internet Applications Information Services (2022); and
- Measures for the Administration of Short Mobile Message Services (2026).

AI and Digital Services Regulation

- Interim Measures for the Management of Generative Artificial Intelligence Services (2023)
- AI-Generated Synthetic Content Labelling Methods (2025)
- Measures for the Management of Anthropomorphic AI Interactive Services (2026)
- AI Technology Ethics Review and Service Measures (Trial) (2026)
- Opinions on the Standardized Application and Innovative Development of Intelligent Agents (2026)
- Digital Virtual Human Information Service Management Measures (draft for comment, 2026) ; and
- Internet Information Service Management Measures (revised draft for comment, 2026)

Law stated - 15 August 2026

Regulatory bodies

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

The Department of Electronic Commerce and Information Technology of the Ministry of Commerce

- Formulating China's E-commerce development plan;
- Promulgating policies and measures to promote digital transformation; and
- Use of e-commerce to open up domestic and foreign markets.

Cyberspace Administration of China (CAC)/Central Cyberspace Affairs Commission (CCAC)

- Overseeing and managing digital content, data security, and personal information protection;
- Managing cybersecurity reviews;
- Organising security assessments for cross-border data transfers;
- Establishing personal information protection certifications; and
- Formulating standard contracts for cross-border personal information transfers.

The Ministry of Industry and Information Technology (MIIT)

-

Coordinating and maintaining national data security and developing the national data security assurance system;

- Coordinating responses to major cyberspace security incidents; and
- Responsible for internet access and telecommunications.

The Ministry of Public Security

- Regulating activities that endanger cybersecurity, cybercrime, and illegal activities involving the unauthorised acquisition and provision of personal information;
- Conducting data security supervision within its power;
- Regulating the installation of malicious software; and
- Disposal of illegal information.

State Administration for Market Regulation

- Managing data security certifications to regulate business practices; and
- Enforcing the E-Commerce Law.

National Data Administration

- Promoting data integration, sharing, and utilisation to foster the development of China's digital economy; and
- Working in coordination with the Cyberspace administration of China to balance security and development, with a focus on digital development.

Law stated - 15 August 2026

Jurisdiction

- 4 | 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?

For foreign-related disputes, including internet-related transactions or disputes, the courts will apply the [Civil Procedure Law](#) and [Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law \(Amendment 2022\) \(the Interpretation\)](#) and [Law on the Application of Law to Foreign-Related Civil Relations](#) to make decisions.

As stipulated in the Interpretation of the Civil Procedure Law, the parties involved can reach a consensus on the choice of jurisdiction of a foreign court in the place where the dispute is associated, as long as the choice of forum does not conflict with the provisions on court-level jurisdiction and exclusive jurisdiction.

In the absence of a choice of the parties, the jurisdiction should be determined in accordance with the provisions of the Civil Procedure Law and the Interpretation. For example, with respect to a contract dispute, the competent court shall be the people's court at the place where the defendant is domiciled or where the contract is performed.

The place of performance is further clarified by the Interpretation. If the subject matter is payment of money, the place where the party receiving the money is located shall be the place where the contract is performed; if the subject matter is delivery of immovable property, the place where the immovable property is located shall be the place where the contract is performed; as for any other subject matter, the place where the party fulfilling obligations is located shall be the place where the contract is performed. As for a contract with instant settlement, the place of transaction shall be the place where the contract is performed.

With regard to an online sales contract, when the subject matter is delivered through the internet, the place where the buyer is domiciled shall be the place of performance; if the subject matter is delivered by other means, the place of receipt is the place where the contract is performed.

In the event that an online contract expressly states that laws of a foreign jurisdiction govern the contract, PRC law may still be applicable in procedural issues. Article 4 of Law on the Application of Law to Foreign-Related Civil Relations states that 'if the PRC has mandatory provisions governing foreign-related civil relations, those provisions are directly applicable'. Article 5 provides that if applying foreign law would harm the PRC's public interest, PRC law prevails. Article 9 clarifies that in the event that a foreign law is applicable according to relevant PRC laws, application of such a foreign law does not include choice-of-law rules of such foreign law.

With regard to jurisdiction of an online contract, if such a contract relates to individual consumer contract, even if such a contract expressly provides for a non-PRC court jurisdiction, according to Article 3 of the Minutes of the National Symposium on Foreign-related Commercial and Maritime Trial Work of Courts Nationwide, issued by the Supreme People's Court on 24 January 2022, such a non-PRC court jurisdiction clause may be invalidated if: (1) the clause was included in relevant standard terms and conditions and the consumer has not been reasonably alerted; or (2) even if the consumer has been reasonably alerted with the foreign jurisdiction clause, applying such a foreign jurisdiction will increase unreasonably costs for seeking remedies to the consumer, then PRC courts will support the consumer's request of bringing case in PRC courts to seek remedies.

Law stated - 15 August 2026

Establishing a business

- 5 | 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?

There is no major difference between establishing a digital business and establishing a brick-and-mortar business in China. Most digital business operators in the form of company,

nature person or other organisations shall complete market entity registration formalities, as stipulated in the E-commerce Law. The regulatory and procedural requirements that govern the establishment of digital businesses are as follows.

Choosing business vehicles

To establish a business in China, the first question to be considered should be which business vehicles to choose. The main business vehicles in China include limited liability company, partnership and company limited by shares. As for foreign enterprises, establishing a representative office instead of a separate legal entity is also available. Nevertheless, a representative office is not able to conduct profitable activities and can only perform auxiliary functions for the parent company.

Pre-examination and approval procedures

The second step is to confirm whether the enterprise needs to go through the pre-examination and approval procedures. The pre-examination and approval procedures include three considerations:

1. whether or not the project involves approval or filing according to the Administrative Measures on Approval and Filing for Foreign Investment Projects, and the Catalogue of Investment Projects Subject to Governmental Approval;
2. whether or not the project is restricted in the Administrative Measures (Negative List) for Foreign Investment Access; and
3. whether or not the licence for conducting business in specific industry is required from the competent authority in charge of the industry.

In accordance with the Negative List 2024 where the restriction on manufacture industry is entirely abolished, foreign investment on digital business is free to enter into China. Nevertheless, the competition of Chinese digital business is widely known to be intensively fierce.

Business registration

The business vehicle shall be registered at the Administration of Market Regulation with all incorporation documents duly signed and submitted. It will be able to conduct commercial activities when the business license is granted. In addition, the digital businesses shall give attention to laws and regulations regarding data compliance and E-commerce, which differs from physical businesses.

Law stated - 15 August 2026

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?

In general, parties can conclude a contract electronically in China. According to article 469 of [the Civil Code](#), the parties may conclude a contract in writing, orally or in some other form. Any electronic data that can show, in material form, the contents that it specifies through electronic data exchange or email and can be accessed for reference and used at any time shall be regarded as a written form. In accordance with article 491 of the Civil Code, where the parties conclude a contract in the form of electronic data and subject to the execution of a letter of confirmation, the contract shall be established at the time of execution of the letter of confirmation. Where the information of any commodity or service released by one party via the internet or any other information network meets the conditions of offer, the contract shall be established when the other party selects such commodity or service and submits the order successfully, unless otherwise agreed by the parties.

Only certain types of contracts cannot be concluded or executed electronically, such as documents involving personal relationships (marriage, adoption and succession), suspension of public services such as water, heat and gas supply, etc. and any other circumstances whereby electronic documents are not applicable as stipulated by laws and administrative regulations.

If the contract is an online sales contract, a click-to-accept process can be adopted. As long as the online contract does not violate the provisions on validity of contract under Chinese law and is deemed a legally valid contract, the contract can be enforced in China. For example, where a term in a contract unconditionally restricts the rights and interests of the parties to a 'click-wrap' contract, the term might be deemed unenforceable.

Law stated - 15 August 2026

Applicable laws

7 | 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?

There are no specific laws in China limiting the choice of governing law or the language of the digital contract. For the forum for disputes, articles 60, 63, 73 of the E-Commerce Law collectively stipulate the forums for digital business contracts disputes.

According to article 60 and article 63, such disputes can be solved through:

- negotiation and mediation by consumer organisations, industry associations, or other legally established mediation bodies;
- filing complaints with relevant authorities;
- arbitration;
- litigation; and
- online dispute resolution mechanism established by E-commerce platform operators.

Regarding foreign-related digital business, article 73 promotes the establishment of cross-border E-commerce dispute resolution mechanisms between different countries and regions.

Notably, the Implementation Rules of Consumer Rights and Interests Protection Law sets further restrictions on the standard form contracts between business operators and consumers. Article 17 prevents business from using the standard terms to unreasonably restrict consumers to choose litigation or arbitration to resolve consumer disputes.

Law stated - 15 August 2026

Electronic signatures

8 | 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?

In China, the [Electronic Signature Law](#) mainly regulates the conduct of electronic signature and confirms the legal validity of electronic signature. Parties involved in civil activities may agree to use, or not to use, electronic signature and data telex for contracts or other documents and instruments.

Electronic signature usually refers to data incorporated into or associated with any electronic form, which may be used to identify the signatory and indicate the signatory's approval of the information contained in the data telex. 'Data telex' means information generated, sent, received or stored by electronic, optical, magnetic or similar items.

Paragraph 1 of article 13 of the Electronic Signature Law provides that an electronic signature can be regarded as a reliable electronic signature if it simultaneously meets all of the following conditions:

- the electronic signature creation data, when used for the electronic signature, is proprietary to the electronic signatory;
- at the time of signing, the electronic signature creation data is only under the control of the electronic signatory;
- any alterations to the electronic signature after signing are capable of being detected; and
- any changes to the content and form of the data message after signature are capable of being detected.

Electronic signatures have the same legal validity as wet-inked signatures or affixation of seal, provided that the electronic signature has satisfied the conditions provided by law. Documents for which the parties involved agree to the use of electronic signature or data telex shall not be denied of legal validity on the ground of electronic signature or data telex being used. However, e-signatures cannot be used in documents or instruments related to personal relationships, conveyance of real estate and stay of public services.

There is no provision stating that digital or e-signature providers must be registered or licensed.

At present, Chinese laws only regulate the form, function and effect of electronic signatures without specifying the specific technical means. Therefore, there is no unique format for electronic signature.

Law stated - 15 August 2026

Breach

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

Special Forums

According to articles 60 and 63 of the E-Commerce Law , apart from initiating litigations or arbitrations, consumers can also seek mediation with the help of consumer organisations, industry associations, or other legally established mediation bodies. Online dispute resolution mechanism will also be applicable if it is provided by E-commerce platform operators.

Remedies

Common remedies for breach of both electronic and offline contracts are the same, including damages compensation, permanent injunctions and specific performance.

Law stated - 15 August 2026

FINANCIAL SERVICES

Regulation

- 10 | 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?

Advertising and selling of financial services products to consumers or businesses digitally or via the internet is also regulated through some key provisions in related laws and regulations.

Regulation on Advertising Financial Services Products

General Legal Provisions

China's current financial advertising regulation system operates under the framework of financial consumer protection. Generally, the Advertising Law, Consumer Protection Law, and Anti-Unfair Competition Law address false advertising or misleading promotion. Ads must be truthful and lawful, avoiding deceptive or misleading content. While these laws

do not specifically mention "financial advertising," financial ads must comply with these general legal requirements.

Given the nature of financial products, marketing often emphasises returns and benefits, potentially neglecting risk warnings. Article 25 of the Advertising Law mandates reasonable risk warnings and prohibitions against guarantees of future results, returns, or risk-free promises, unless specified otherwise by the state. It also prohibits endorsements or certifications by academic institutions, industry associations, professionals, or beneficiaries.

Article 28 of the Consumer Protection Law outlines disclosure obligations for specific sectors, including providers of securities, insurance, and banking services. They must provide consumers with information on operational addresses, contact details, product or service quantity and quality, prices or fees, performance terms, safety precautions, risk warnings, after-sales service, and civil liability. This provision protects financial consumers' right to information and binds financial service providers to disclosure and risk warning duties.

Article 8 of the Anti-Unfair Competition Law prohibits operators from engaging in false or misleading commercial promotion regarding their products' performance, features, quality, sales status, user reviews, or honours. It also forbids facilitating false or misleading promotions through fake transactions.

Industry Regulatory Requirements

China's current laws do not explicitly define 'financial advertising'. Relevant provisions appear in various financial sector regulations and normative documents, generally as principles or indirect rules.

For example, the Regulations on the Administration of Securities Issuance and Underwriting prohibit issuers and lead underwriters from conducting false or misleading advertising or promotional activities. Article 45 of the Regulations on Insurance Company Management requires insurance institutions to disclose information according to regulations and prohibits misleading advertising about insurance terms and service quality. Articles 16, and 45 of the Measures for Supervision and Administration of Sales Agencies for Publicly-offered Securities Investment Funds address illegal production, distribution, or publication of fund promotional materials, indirectly regulating fund advertising. The Regulations on the Supervision and Administration of Commercial Bank Wealth Management Business mandates comprehensive, truthful, and objective disclosure of wealth management products' key features, investment portfolios, valuation methods, custody arrangements, risks, and fees. The language used must be accurate and clear.

Regulations on Selling Financial Service Products

On 21 April 2026, the Measures for the Online Marketing of Financial Products (Measures) was officially issued and will take effect on 30 September 2026. The Measures represent the first comprehensive regulatory framework unifying the online marketing rules for all types of financial products, covering deposits, loans, securities, asset management products, insurance, precious metals (excluding physical precious metals), foreign exchange products, futures, derivatives, payment services, and investment advisory or

consulting services. It applies to both financial institutions and third party internet platforms engaged by financial institutions, while explicitly prohibiting any unlicensed entity from conducting or disguising financial product marketing.

The Measures set clear compliance boundaries that financial institutions bear primary responsibility for marketing content, shall set up head office level review mechanisms, and ensure all promotional materials are accurate and not misleading. Platforms may only provide technical forwarding services and must redirect users to the institutions' own platforms before any purchase or service use. The rules also ban a range of deceptive practices such as guaranteeing returns, using short term performance to mislead, promoting instalments by hiding total costs, or employing enticing phrases like "low risk" or "high yield". Payment institutions may not list loans or wealth products as payment options, and bundled sales cannot be default checked.

Additionally, the Opinions on Promoting the Regulated, Healthy, and Sustainable Development of the Platform Economy (referred to as the 'Opinions') focus on improving the governance system for the platform economy. In terms of financial regulation, the Opinions strengthen supervision in the payment sector by concentrating oversight on the abuse of market dominance in non-bank payment services and exploring the introduction of regulations for non-bank payment institutions. The Opinions also strictly regulate platform enterprises' investments in financial institutions and local financial organisations, while enhancing the financial consumer protection mechanism to prevent the promotion of premature consumption.

Measures for the Suitability Management of Financial Institution Products promulgated in July 2025 further amplifies that financial institutions shall clarify and access the standards for identifying private placement product investors while selling private placement products.

Data security requirements for Financial Services

The Measures for Data Security of Banking and Insurance Institutions, issued by the National Financial Regulatory Administration on 27 December 2024, impose comprehensive data security obligations on banking and insurance institutions. Institutions must establish a governance system covering the full data life cycle, classify data into core, important, and general categories, and implement differentiated protections. Prior to processing sensitive-level data or engaging in significant activities such as entrustment, sharing, or cross-border transfer, institutions must conduct a data security assessment. The Measures require a "firewall" between parent banks/groups and subsidiaries for data sharing, which requires data subject consent for sharing sensitive data. Cross-border transfers of important data and personal information require security assessments under national policies. Personal information must be collected only to the minimum extent necessary for business purposes, under the principle of clear notification and authorised consent, and institutions may not refuse services solely because a customer withholds consent unless the processing is essential to the service.

Law stated - 15 August 2026

Electronic money and digital assets

I

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

Electronic banking

The Electronic Payment Guidelines (No. 1), promulgated by the People's Bank of China (PBOC), is the first document that sets out banks' liability regarding online payment. The Measures for Management of Electronic Banking and the Guidance on Evaluation of Electronic Banking Security issued by the China Banking and Insurance Regulatory Commission generally govern the electronic banking business.

Third-party payment

Third-party payment operators are defined as non-bank institutions that handle internet payments, mobile phone payments, fixed-line payments, digital television payments and other network payment services.

The regulator of third-party payment is the PBOC and its branches. The core of the policy is the Regulation on Supervision and Administration of Non-bank Payment Institutions and its implementing rules, supplemented by industry self-regulation and supervision by commercial banks. Due to the rapid development of third-party payments, the PBOC has introduced more policies to regulate third-party payments since 2014.

The promulgation of the E-Commerce Law in 2019 brought new requirements to electronic payment service providers, including requirements to:

1. notify users of the functions of electronic payment services, use methods, points to note, the relevant risks and fee rates, etc;
2. not impose unreasonable transaction conditions;
3. ensure the integrity, consistency, trackability and resistance against tampering of electronic payment instructions;
4. provide account reconciliation service and transaction records of the past three years to users free of charge;
5. promptly investigate and identify the reason for errors in payment instructions, and adopt the relevant measures to correct the error; and
6. bear compensation liability where an error causes the user to suffer losses, except where it can be proven that the error in the payment instruction was not caused by the electronic payment service provider.

Digital Currencies and Virtual Currencies

In China, digital currency (e-CNY) refers to the digital form of legal tender issued by the PBOC. It is primarily intended as a substitute for physical currencies, operated by designated institutions, and exchanged with the public. The currency is paid electronically and holds the same value as paper currency. The Central Bank Digital Currency (CBDC) is categorised into wholesale CBDC, aimed at institutions like commercial banks for large-scale settlements, and retail CBDC, intended for public use in daily transactions. By 28 March 2024, the digital yuan has been put into experimental use in 26 areas across 17 provinces in China, with transaction volumes steadily increasing.

On 5 December 2013, five regulatory bodies, including the PBOC and the China Banking Regulatory Commission, issued the Notice on Preventing Bitcoin Risks. This document defined Bitcoin as a virtual commodity and explicitly stated that it does not have the same legal status as currency and should not be used as currency in the market. Financial and payment institutions, including banks, are prohibited from engaging in Bitcoin transactions. Digital exchanges must register with government telecom regulators and comply with anti-money laundering regulations.

On 4 September 2017, seven regulatory bodies, including the PBOC and the Cyberspace Administration of China, jointly issued the Announcement on Preventing Token Issuance and Financing Risks. The announcement declared Initial Coin Offerings (ICOs) to be unauthorised and illegal fundraising activities. It ordered all types of ICOs to immediately cease and instructed that all assets held in investor accounts be returned promptly.

On 24 September 2021, ten regulatory bodies, including the PBOC and the China Banking and China Securities Regulatory Commission, issued the Notice on Further Preventing and Handling the Risks of Virtual Currency Trading and Speculation. This notice stated that 'virtual currencies like Bitcoin and Ether do not have the same legal status as legal tender and cannot be circulated as currency in the market.' It classified virtual currency-related business activities as illegal financial activities that must be strictly banned. Concurrently, the National Development and Reform Commission issued a notice on its website banning all forms of cryptocurrency mining activities, including those under different names, categorising them as an industry to be eliminated, and halting all financial and tax support for them.

Law stated - 15 August 2026

Digital and crypto wallets

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

China has a strictly prohibitive attitude towards the issuance and trading of crypto currencies. Financial institutes are forbidden from engaging in financing services and exchange of crypto currencies.

In the meantime, domestic digital payment system allows digital deposits which facilitate existence of e-wallet. The PBOC regards the e CNY wallet as a parallel system to bank accounts or 'digital safes', without interest accrual and not subject to normal deposit laws; it is fully backed by the national fiat currency unit and under tight state control.

Since September 2021, the PBOC declared 'virtual currency related financial services' (including wallets, exchanges, derivatives, ICOs, trading platforms) as illegal financial activities and subject to criminal investigation. This includes both domestic and offshore providers serving mainland users. Private individuals are not prosecuted simply for holding crypto as a digital commodity, but any use involving trading, payments, or exchanges is illegal.

In March 2025, although a Shanghai court recognised crypto assets as property under Chinese civil law, allowing ownership, but upheld the ban on use in financial or commercial activities within the PRC.

Law stated - 15 August 2026

Electronic payment systems

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

There are mainly two types of electronic payments in China: online banking payment and third-party payment (Alipay, WeChat). Online banking payment is regulated by [the Electronic Payment Guidelines \(No. 1\)](#) issued by the People's Bank of China in 2005 and a draft amendment on the Electronic Payment Guidelines (No.1) was proposed and open for comment in August 2025. The guidance clarifies the obligations of banks when using electronic payment (which include the application of electronic payment, the initiation and receipt of electronic payment instructions and the measures of safety control and error handling).

Third-party payment like Alipay and WeChat is in widespread use from metropolis to remote countryside in China. Third-party payment institutions are now under the regulation of the People's Bank of China and its subordinate units. In 2017, the People's Bank of China issued a total of 106 administrative penalty decisions against third-party payment institutions, many of whom were blamed for not being adherent to the administrative measures issued by the People's Bank of China. Moreover, The Regulations on the Supervision and Administration of Non-Bank Payment Institutions, issued by the Ministry of Justice and the People's Bank of China, took effect on 1 May 2024. With respect to the conditions for third party payment institutions like Alipay, Wechat Payment carrying business and their business practices, the Regulation specify the licensing and entry requirements, rules on business rules and risk management, user rights protection and penalties for violations.

Third-party access to digital information in bank accounts is subject to regulation under the Civil Code, the Personal Information Protection Law, the Commercial Banking Law and [the Consumer Rights and Interests Protection Law](#), as well as departmental regulations such as [the Implementation Measures of the People's Bank of China on the Protection of the Rights and Interests of Financial Consumers](#). Third-party access to personal bank account information requires the individual's consent, with the exception of requirements by law-enforcement departments.

In addition to the laws, the Technical Specification for the Protection of Personal Financial Information provides a technical standard for financial institutions entrusting the processing of personal financial information to third parties. It stipulates that the entrustment should not exceed the scope of the consent of the subject of the personal financial information. And it places more detailed demands on the entrusted third-party institution.

Law stated - 15 August 2026

Online identity

- 14** | 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?

Pursuant to the [China Anti-Money Laundering Law](#), where a financial institution determines the identity of a customer through a third party, it shall ensure that the third party has adopted measures for determining customer identity complying with the requirements of this Law. And where the third party has not adopted measures for determining customer identity that comply with the requirements of this Law, the financial institution shall bear the liability of not fulfilling the obligation of determining customer identity. Generally, Chinese law permits the use of third parties to satisfy KYC requirements. The Administrative Measures for Financial Institutions on Customer Due Diligence and Keeping of Customer Identity Information and Transaction Records released in 2022 clearly outlined the conditions under which financial institutions may delegate KYC services to third parties. Additionally, the regulation stipulates that the financial institutions remain liable for failing to fulfil their customer identification obligations. In 2022, the People's Bank of China released a regulation requiring financial institutions to assess third parties' risk status and ability to perform the obligations of AML and counter-terrorist financing.

Nevertheless, when it comes to customer identity for credit card applications, the Notice on Further Promoting the Standardised and Healthy Development of Credit Card Business promulgated by the China Banking and Insurance Regulatory Commission and the People's Bank of China stipulates that banking financial institutions shall accept credit card applications, collect customer information and verify customers' identities via their own channels, instead of relying on an internet platform, webpage or any other electronic channel operated or controlled by any cooperative agent. In cases of inquiries regarding bills or payables via the aforesaid electronic channels, prior consent should be obtained from customers and necessary measures must be taken to ensure the security of customers' personal information.

Artificial Intelligence in Financial Services

The Guiding Opinions on the Safe Development and Application of Artificial Intelligence in the Banking and Insurance Industry issued on 18 June 2026 establish a comprehensive AI governance framework for financial institutions. Institutions must establish board-level oversight, implement full life cycle management of AI systems, and adopt risk classification for AI applications. High-risk applications involving fund transactions, credit approval, underwriting, and generative AI affecting customer interests require risk committee

approval, with human oversight and backup systems mandatory. The Opinions expressly prohibit using directly identifiable personal information (names, ID numbers, phone numbers, bank card numbers) for generative AI training. AI-generated content must be clearly labelled, and for high-risk scenarios, AI may only serve as an auxiliary tool with human final decision-making. Institutions must also manage outsourcing and supply chain risks and report generative AI use in public-facing or high-risk applications to the National Financial Regulatory Administration.

Law stated - 15 August 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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?

To take ownership of a domain name, applicants for registration shall register (purchase) the possible domain name from the China Internet Network Information Centre (CNNIC) or the qualified registrars accredited by the CNNIC that then shall provide an electronic certification.

There are no filing formalities for domain names in China. However, applicants who use the registered domain name for a website shall fulfil the website filing formalities with the competent department, according to the Administrative Measures on Internet-based Information Services.

It is possible for a resident to register a country-specific domain name in China without that resident being in China. In China, a country-specific domain name refers to a .cn or a . (China) domain name. The Implementing Rules for the Registration of National Top-level Domain Names 2019 provide that no restriction is imposed against non-residents to register a .cn or a . domain name. Additionally, the Ministry of Industry and Information Technology also specifies the permitted registrants, either individuals or entities.

Law stated - 15 August 2026

IP ownership

- 16** | 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?

Domain names and URLs are not the subject of trademark or copyright according to the related laws in China. Note that in amended PRC Trademark Law, China National Intellectual Property Administration (CNIPA) is granted power to proactively revoke registered trademarks that are not in use and explicitly bans registration not for the purpose

of usage in consecutive three years, rendering traditional trademark strategies for unused URLs and domains legally vulnerable.

The [Anti-Unfair Competition Law](#) defines the unauthorised use of the main part of another party's domain name, website name, web page, etc, that is influential as misleading acts, which may cause the public to misidentify the goods concerned as another party's goods or to associate the goods concerned with those of another party. Only domain names or URLs that are influential are protected by the Anti-Unfair Competition Law.

In accordance with the [Interpretations of Several Issues Concerning the Application of Law to the Trial of Civil Dispute Cases Involving Computer Network Domain Names](#) from the PRC Supreme People's Court (SPC), the registration or use of domain names – which includes but is not limited to copying, imitating or translating well-known trademarks or being identical with or similar to registered trademarks or domain names – may also constitute infringement and thus be regulated by [the Trademark Law](#).

However, if the domain misleads the public or unfairly appropriates reputation, the right holder may proceed under the Anti Unfair Competition Law or through domain dispute claims.

For '.cn' domains, as of 1 August 2019, the WIPO Arbitration and Mediation Center provides [domain name dispute resolution services for.cn and. .](#), pursuant to the China ccTLD Dispute Resolution Policy (.cn Policy), the China ccTLD Dispute Resolution Policy Rules (.cn Rules), and the WIPO Supplemental Rules for China ccTLD Dispute Resolution Policy and China ccTLD Dispute Resolution Policy Rules (WIPO Supplemental Rules). The '.cn Policy' allows owners of civil rights (eg, trademarks, business names, product names) to file an administrative complaint for '.cn' domains registered less than three years.

Law stated - 15 August 2026

ADVERTISING

Regulation

17 | What rules govern online advertising?

The governing rules are the following.

- Legislation: [the Advertising Law 2021](#), as amended.
- Administrative regulations:
 - [the Administrative Provisions on Algorithm Recommendation for Internet Info rmation Services 2022](#);
 - [the Administrative Measures for Internet Advertising 2023](#); and
 - [the Provisions on the Governance of Network Information Contents Ecosystem 2019](#).

- [Measures for the Administration of Short Message Services \(2026\)](#)
- Self-regulatory codes: the China Advertising Association is the industrial self-discipline association for advertising, which formulated and promulgated self-regulatory codes for the advertising industry (eg, the Self-Regulation of the China Advertising Association and the Self-Discipline Pact).

Law stated - 15 August 2026

Targeted advertising and online behavioural advertising

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

Online advertising is defined as commercial advertisements that directly or indirectly promote goods or services through websites, web pages, internet applications and other internet media in the forms of texts, pictures, audios, videos, etc.

Online editorial content can be regarded as online advertising provided that there is a paid promotion of goods or services, directly or indirectly, for profit. According to the Advertising Law 2021, commercial advertising shall involve the activities carried out by sellers of goods or service providers to promote their goods or services, directly or indirectly, through a certain medium and form. Therefore, editorial content shall be caught by the rules governing advertising only if it can meet this condition.

With the enlarged application of big data, the techniques of data collection, analysis and application enable business operators to post the targeted advertising and online behavioural advertising. For the first time, the Administrative Measures for Internet Advertising (2023) regulates the use of algorithmic in advertising, and explicitly requires that the advertisement publishing body should put its own rules related to algorithmic recommendations services, advertisement placement records and other documents needed in the advertisement placement records. Otherwise, the violators will possibly face administrative penalties.

Law stated - 15 August 2026

Misleading advertising

- 19** | Are there rules against misleading online advertising?

The rules against misleading online advertising are mainly set forth in Anti-Unfair Competition Law 2019, the Advertising Law 2021 and the Administrative Measures for Internet Advertising 2023.

The 2025 amendment to the Anti-Unfair Competition Law enhances enforcement by increasing maximum fines for misleading marketing to 2 million yuan and removing minimum penalties. This aims to more effectively deter online fraudulent practices.

Under the Advertising Law 2021, a wider variety of advertisements are now vulnerable to scrutiny for false advertising. Advertisers are now required to substantiate all claims and statements regarding their truthfulness to avoid non-compliance. The use of technical or digital methods to create or enhance the true effect of a product or service in advertisements, in particular, is penalised as false advertising.

Article 10 of the Administrative Measures for Internet Advertising 2023 provides that an advertiser who publishes pop-ups advertisements must significantly mark the closure sign to ensure on-click closure, and the closure sign shall not be false or misleading. According to article 11, online advertising is prevented from deceiving or misleading users into clicking on or browsing the advertisements under certain circumstances. Additionally, in accordance with article 13, an advertiser shall be responsible for the truthfulness of the contents of an internet advertisement. An advertiser must establish and regularly update advertising files, which should be retained for at least three years from the date an advertisement is published. The platform operator must verify a third party advertiser's identity, establish advertising files, regularly check and update them, record and preserve relevant electronic data of advertising activities for at least three years, and remove any illegal advertisements.

Law stated - 15 August 2026

Restrictions

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

General rules in the Advertising Law 2021 include that the following shall not be advertised:

1. narcotic drugs;
2. psychotropic substances;
3. toxic drugs for medical use;
4. radioactive pharmaceuticals and other special drugs;
5. drug precursor chemicals; and
6. pharmaceuticals, medical machinery and treatment methods for drug abuse rehabilitation.

Prescription drugs other than those stipulated in the above list may only be advertised in medical or pharmaceutical professional journals that are jointly designated by the health department of the State Council and the drug regulatory department of the State Council.

In accordance with the Administrative Measures for Internet Advertising 2023, the following advertisement shall be prohibited:

- Tobacco (including e-cigarette) ads and prescription drug;
- Medical treatments, drugs, health foods, special dietary foods, medical devices, cosmetics, alcohol, beauty products, and harmful online games on all websites, web pages, apps and public WeChat accounts targeting minors; and

- Medical treatments, drugs, medical devices, health foods, and special dietary foods disguised as health or wellness information online (if health or wellness information is provided, it cannot appear alongside business details, contact information, or purchase links related to these products).

It further clarifies a set of products approved to be advertised online under certain conditions. For example, medical treatments, drugs, medical devices, pesticides, veterinary drugs, health foods, and special dietary foods must not be published online without prior approval.

Law stated - 15 August 2026

Direct email marketing

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

Email, SMS and other distance marketing are supervised by the Regulations on the Administration of Short Message Services, the Administrative Measures for Internet Advertising and the Advertising Law.

Unsolicited marketing is not allowed in China. The Administrative Measures for Internet Advertising and the Advertising Law explicitly prohibit advertisers from attaching advertisements to, or including advertising links in, replies to emails sent by users without their permission.

Under the 2026 Revision of the Short Message Services Measures, SMS service providers must obtain proof of recipient consent before transmitting commercial messages and retain such records. They must also provide a convenient opt-out mechanism with each message; once a recipient explicitly refuses, further transmission is prohibited. Port codes for commercial SMS and service-related SMS may not be mixed. Providers are required to transmit the sender's true identity (full name, abbreviation, or registered trademark) with each message. Basic telecom operators must offer anti-intrusion services to users and strictly fulfill access management responsibilities.

Also, the Advertising Law regulates the sending of advertisements by means of electronic messages, requiring any entity or individual to obtain the consent or request of the person concerned before sending the advertisement, and to provide the recipient with a means to refuse to continue receiving the advertisement after it has been sent. Otherwise, the advertiser shall be subject to administrative liability, which includes orders for corrections and fines.

The Administrative Measures for Internet Advertising further specify that no advertisements or links to advertisements shall be attached to emails or internet instant messaging, and no internet advertisements shall be sent to users' vehicles, navigation devices, smart home appliances, etc, without the consent or request of the person concerned. Otherwise, advertisers, operators and publishers of advertisements shall bear administrative liabilities, which include orders for corrections, confiscation of illegal income and imposition of fines.

Law stated - 15 August 2026

ONLINE PUBLISHING

Hosting liability

- 22** | 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?

Article 45 of the Advertising Law 2021 stipulates that internet information service providers shall curb the posting and publishing of illegal advertisements through their information transmission and distribution platform of which they are aware or should be aware.

For any violation of these provisions, the State Administration for Market Regulation shall confiscate the illegal income. Where the amount of the illegal income is 50,000 yuan or above, a fine ranging from one to three times the amount of the illegal income shall be imposed simultaneously. Where the amount of the illegal income is less than 50,000 yuan, a fine ranging from 10,000 to 50,000 yuan shall be imposed simultaneously. In serious cases, the relevant authorities shall order the offender to stop the relevant businesses.

Article 1195 of the Civil Code states that when a network user commits an infringement using network services, the rights holder has the right to notify the internet service provider to take necessary measures such as deleting content, blocking access, or disconnecting links. Upon receiving the notification, the service provider must promptly forward it to the relevant user and take appropriate actions based on preliminary evidence of infringement and the type of service provided. If the provider fails to act promptly, they shall be held joint liability with the user for any additional harm caused.

Article 1197 of the Civil Code further stipulates that if an internet service provider knows or should know that a user is using their service to infringe on others' civil rights and fails to take necessary measures, the provider shares joint liability with the user.

According to article 41 of the Anti-Telecom and Online Fraud Law, telecommunication and internet service providers who violate the law by failing to perform duties such as verification, real-name registration, or monitoring, may face administrative fines. Authorities may also order them to suspend relevant services, cease operations, shut down websites or applications, or revoke business licenses. In severe cases, the providers may face criminal charges for 'refusal to perform security management obligations' or 'assisting in criminal activities related to information networks' under the Criminal Law. The National Cybersecurity Incident Reporting Management Measures effective on 1 November 2025 imposes additional reporting obligations on network operators for cybersecurity incidents.

Based on the above, these providers should fulfil their obligations related to information verification, security management, and due diligence to avoid legal liability.

Law stated - 15 August 2026

Content liability

- 23** |

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?

The internet service provider (ISP) shall not bear liability for infringement when the relevant copyright owner fails to issue a warning or provide any other information that is sufficient to make the ISP aware of such an infringement. The necessary measures taken by the ISP include the technical approaches that may directly prevent the occurrence of infringement consequences, such as deleting infringing content, breaking links and filtering keywords.

After receiving the notice, if the ISP still does not remove the infringing link within a reasonable period resulting in the further expansion of the damage, it will bear the legal responsibility for such additional damages.

Platforms that hold an 'Internet News Information Service License' (eg, Weibo public account operator, content-rich websites, livestream hosts) are subject to stricter standards. Under the Internet News Information Service Management Regulations amended in 2024, licensed publishers must maintain editorial and fact checking systems and correct or remove any inaccurate statements that harm subjects' interest.

Internet information services providers are obliged to ensure that no illegal content (including rumours, defamation, extremist messages) is published and must remove relevant content immediately if the relevant online information service provider discover such content and report to relevant authorities under articles 15 and 16 of the Internet Information Service Management Measures and the Content Ecosystem Governance Regulations.

Internet content service providers must publicise their ICP (Internet Content Provider) license or Internet News License number prominently on the homepage.

Law stated - 15 August 2026

Shutdown and takedown

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

Shutting down a web page containing defamatory material could be one of the requisite measures according to article 1,195 of the Civil Code. It is an ISP's obligation to take requisite measures if the injured party sends a notice of infringement to the ISP, providing the preliminary evidence of infringement and its true identity information. With respect to which specific requisite measure or measures shall be taken, the ISP shall, based on the preliminary evidence for infringement and the type of services, make the decision accordingly.

Law stated - 15 August 2026

INTELLECTUAL PROPERTY

Data and databases

25 | Are data and databases protected by IP rights?

There is no express law that stipulates that all data and databases are protected by IP law. In general, only the data and databases formulated or perceived in an original manner can be granted copyright and thus protected. In accordance with article 127 of the Civil Code, data and internet virtual property are protected based on other regulations, if any. Generally, data and databases are not the objects of civil rights in Chinese law, and have limited protection as objects of IP rights. The Anti-Unfair Competition Law offers protection as data and databases can be defined as trade secrets, trademarks, etc. The Data Property Rights Registration Work Guidelines (Trial) provides a registration-based mechanism for establishing data ownership, which may serve as evidence of rights in IP-related disputes.

Law stated - 15 August 2026

Third-party links and content

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

Legal practice in China deems that the link itself does not contain any content and therefore is not subject to the control of the right to network dissemination of information. The Supreme People's Court published [the Provisions on Several Issues Concerning the Application of Law to Trial of Civil Dispute Cases of Infringement of the Right to Network Dissemination of Information](#), stipulating that the internet service provider (ISP) whose conduct constitutes joint infringement with other parties shall bear joint and several liabilities, but also providing an exemption for the ISP if it only provides a link.

However, for built-in deep linking behaviour, it is a different case. Deep linking is a technical means that allows users to directly see the content of the linked website on the linking website without a web page transition. In Chinese legal practice, the 'sever standard' has been gradually adopted when deciding whether there is an infringement on copyright in such cases. Meanwhile, the Anti-unfair Competition Law is referred to as a supplement to the copyright law when it constitutes misconduct hereunder.

Law stated - 15 August 2026

27 | 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?

Where a network user or an ISP provides works, performances, and audio and video products via an information network without the permission of the right holder for network dissemination of information, such provisions shall be deemed an infringement of the rights to network dissemination of information. Meanwhile, making available works,

performances, and audio and video products in the information network by means of uploading to a network server, setting up shared files or using file-sharing software, etc, that enables the general public to download, browse or by other means obtain them at any desired time and location shall be deemed constitutions of the aforesaid provisions.

Law stated - 15 August 2026

Metaverse and online platforms

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

The legislation for the metaverse and virtual property is still under development. At the current stage, intellectual property protection in the metaverse faces a few difficulties. The Digital Virtual Human Information Service Management Measures (draft for comment) and the Opinions on the Standardized Application and Innovative Development of Intelligent Agents signal increasing regulatory attention to virtual and agentic environments.

First, the rules for evidence collection and burden of proof concerning infringement of intellectual property rights (IPR) in the metaverse are unclear. For instance in commercial practice, virtual reality (VR) service providers usually only conduct formal review and ignore substantive review, leading to the problem of copyright infringement where many VR applications are copied illegally.

Second, the general laws applied for IPR infringement may become inapplicable for IPR infringement in the metaverse. For example, 'without the consent of the trademark registrant, replaces his registered trademark and puts the goods with the replaced trademark back on the market' is stipulated as an act of trademark infringement according to the Trademark Law. However, it becomes difficult to identify such acts since only virtual products, not physical objects, exist in the metaverse.

Third, according to the current IPR protection law system, a trademark is only protected within the territory where the trademark is registered. However, in the metaverse, the territoriality of IPR protection may be challenged.

Law stated - 15 August 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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?

The principle of exhaustion of rights has been recognised by PRC law in some areas.

For example, in new plant variety rights protection, the Supreme People's Court proposed that, after the variety right-holder authorises or licenses the plant variety material to be sold, it shall not claim that the production, propagation or sale of such plant material by others constitutes infringement (exceptions apply). Similarly, the PRC patent law stipulates

that once the patented products are sold by the patentee or its licensee, the use, offer for sale, sale and importation of such products no longer constitute infringement of the patent right.

Regarding digital products, the Copyright Law and Regulations on Computer Software both indicate that for legally distributed copies of software, the right-owner's distribution right has been exhausted.

In April 2022, the PRC's first non-fungible token (NFT) infringement case was decided by Hangzhou Internet Court. The judgment denied application of the principle of exhaustion of rights for NFT digital products. It reasoned that the principle is based on the inseparability of the work itself and its tangible carrier. Since the distribution of NFT digital works does not lead to the distribution of their tangible carriers, NFT digital works do not meet the prerequisite to apply the exhaustion of rights principle.

In addition, the original purpose of the exhaustion of rights principle is to balance the conflict of interests between the copyright owner and the legitimate buyer, but NFT digital works can be copied without cost and in unlimited quantities, so unauthorised duplicates and distribution would seriously harm the interests of the copyright owner.

This case is a preliminary exploration of Chinese justice in the field of the metaverse. As discussion over the topic grows, more authoritative legislation is expected in the near future.

Law stated - 15 August 2026

Administrative enforcement

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

The term 'dawn raid' is not directly incorporated into Chinese law, but the most similar existing concepts are administrative or criminal investigations (inspections), which allow law enforcement to conduct on-site inspections as well as search corporate records and files to gather information and evidence on suspected violations of law.

In administrative procedures, which are usually initiated by a complaint filed by the IP right holder, the competent administrative authorities – such as the Copyright Bureau in a case of copyright infringement – do not have the power to issue a freezing injunction. However, in terms of dawn raids, the administrative authorities may, when investigating the suspected infringement;

1. question the relevant parties;
2. investigate the matters relating to the alleged illegal acts;
3. conduct on-site inspections of premises and articles of the parties concerned that involve alleged illegal acts;
4. inspect and make copies of contracts, invoices, account books and other relevant materials relating to the alleged illegal acts; and
5. seal up or seize the premises and articles involving the alleged illegal acts.

Law stated - 15 August 2026

Civil remedies

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

Civil remedies rendered in a civil judgement may include ordering the infringers to stop infringement, eliminate impact, apologise or compensations to IP owners.

Search orders and freezing injunctions are available under different circumstances.

There are two types of injunctions issued by the court, ordering the infringing party to perform or refrain from certain actions for consideration:

- Injunctions to stop infringement before the litigation.
- Injunctions to stop infringement during the litigation.

When applying for injunctions, the party shall provide guarantee accordingly. The party may apply for reconsideration to the court if the injunction application is dismissed by the court at the first time.

In addition, the court may order the infringing party to immediately stop infringement in the formal and final judgment. When the facts are clear, a partial judgment may be made prior to the final judgement ordering for cessation of infringement. The order issued in a judgment can only be challenged by appealing to higher court.

After the civil judgment comes into effect, the IP owner may file an application for enforcement with the enforcement division of the court.

If the infringer does not perform the obligations ordered in the civil judgment, the court shall have the right to enquire about the infringer's properties and issue freezing injunctions. If the infringer does not perform the obligations ordered in the civil judgment and conceals its properties, the court shall have the right to issue a search order signed by the president of the court. The court shall also have the right to conduct a search on the infringer and its residence or the place where the property is concealed.

Law stated - 15 August 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

32 | 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 Information Protection Law (PIPL), effective as of 1 November 2021, defines personal information and personal data as:

all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously. The processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.

Sensitive personal information refers to the personal information that is likely to result in damage to the personal dignity of any natural person, or damage to his or her personal or property safety once disclosed or illegally used, including information such as biometric identification, religious belief, specific identity, medical health, financial account, whereabouts and previous location history, as well as the personal information of minors under the age of 14.

Additional rules apply to the processing of sensitive personal data including, subject to the individual's separate consent (written consent is required in some cases), the need to inform the individual of the necessity of processing his or her sensitive personal information and the impact on his or her personal rights and interests. The consent of a minor's parents or other guardians in the case of processing the personal information of a minor under the age of 14 must be obtained.

Information processed anonymously is currently not regulated.

Law stated - 15 August 2026

Registration and appointment of data protection officer

- 33** | 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?

The Cyberspace Administration of China (CAC) is the competent authority for leading and coordinating the supervision of personal information processors. Meanwhile, other government departments including the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation (SAMR) are responsible for protecting, supervising and administering the protection of personal data within the scope of their respective duties. Currently, there is no regulatory registration system designed for personal information processors. However, this does not mean personal information processors in China can avoid supervision.

The Personal Information Security Standards 2020 regulate the personal information protection officer system. Where a personal information processor meets any of the below thresholds, it shall designate a personal information protection officer:

1. if it processes personal information as its main business and has more than 200 employees;
2. if it processes the personal information of more than one million people or expects to process the personal information of more than one million people within the next 12 months; or

3. if it handles the sensitive personal information of more than 100,000 people.

Additionally, on 4 November 2022, the Cyberspace Administration of China and the State Administration for Market Regulation issued and implemented the Personal Information Protection Certification Implementation Rules, which state that personal information processors engaged in cross-border processing activities shall meet the specific requirements in the Security Certification Specifications for Personal Information Cross-border Processing, which provides detailed instructions for personal data processors engaged in cross-border activities. It stipulates that both the personal information processors engaged in cross-border activities and its overseas recipients, shall appoint either a person in charge from the decision-making body who has expertise in personal information protection and relevant management skills or a department to perform protection obligations, preventing unauthorised access and avoiding leaks, alterations, or loss of personal information.

The Large Network Platform Personal Information Protection Regulations (draft for comment) proposes additional requirements that the data protection officer shall be a member of senior management, holding Chinese nationality and have no permanent residency or long-term residence abroad, with at least five years of relevant experience, with veto power over personal information processing matters.

Law stated - 15 August 2026

Extraterritorial issues

- 34** | 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 PIPL shall apply to all processing activities of personal information that occur in China. The PIPL also applies to the processing activities of personal information that occur outside China if:

1. the purpose of such processing activity is to provide products or services to a natural person within China; or
2. the activities of the natural person within China are analysed and evaluated.

Where a personal information processor needs to transfer personal data outside China, it shall conduct the data protection impact assessment (DPIA) in advance, and apply one of the following mechanisms depending on the type of personal data processed, the volume of personal data processed on whether it has met specific thresholds on a case-by-case basis::

1. get the certificate issued by a specialised agency appointed by the CAC;
2. pass the security evaluation organised by the CAC; or
- 3.

enter into a contract with the overseas recipient under the standard contract formulated by the CAC.

In addition, the personal information processor shall take necessary measures to ensure that the overseas recipient also satisfies Chinese standards.

Foreign national residents within China will also be protected by the PIPL.

Law stated - 15 August 2026

Bases for processing

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

With globalisation and the booming of the internet economy, there are many scenarios in which enterprises transfer domestic personal information across borders to foreign countries. The following are the most commonly seen:

1. global enterprises require their subsidiaries, branches or representative offices in the PRC to transfer management information, such as personal information of employees, to the headquarters abroad;
2. companies collect personal information during business operations in the PRC, and then share it with their foreign parent companies;
3. cross-border e-commerce operators store personal information on servers outside the PRC, or outsource their personal information processing to companies abroad;
4. cross-border service providers, such as of insurance, medical care, tourism and study consultancy, collect personal information in the PRC and store it on a server abroad or provide it to foreign companies; and
5. enterprises provide investigation and evidentiary materials involving personal information to offshore government departments and parent companies, for the purpose of anti-fraud investigations, offshore litigation and arbitration bodies.

Law stated - 15 August 2026

Data export and data sovereignty

36 | 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?

Formulated specifically for the regulation of data export, the Security Assessment Measures for Outbound Data Transfers came into effect on 1 September 2022. Meanwhile, the Personal Information Protection Law, Data Security Law and Cybersecurity Law

supervise the export or transfer of personal data to another jurisdiction. Based on these laws and regulations, China's current data export regulation system includes the following three methods:

1. Security Assessment organised by the Cyberspace Administration of China (CAC), applicable to the following data processors:
 - Operators of critical information infrastructure providing important data or personal information overseas;
 - Data processors providing important data overseas; and
 - Data processors processing personal information that meets the quantity threshold set by the CAC.

Important data refers to data that, if altered, destroyed, disclosed, illegally obtained, or misused, could jeopardise national security, economic operations, social stability, public health, or safety. The data processor meeting the quantity threshold refers to data processors handling personal information of over 1 million individuals and those who have provided personal information of 100,000 individuals or 10,000 sensitive individuals to overseas entities since 1 January of the preceding year.

2. Personal Information Protection Certification: Conducted by professional institutions The Personal Information Export Certification Measures further refines the certification pathway and GB/T 46068-2025 (Data Security Technology – Security Certification Requirements for Cross-border Personal Information Processing Activities serves as the core certification standard.

3. Standard Contract for Personal Information Export: Signed between the data processor and the overseas recipient of personal information.

Under the Security Assessment Measures for Outbound Data Transfers, to provide data abroad under any of the following circumstances, a data processor must declare a security assessment for its outbound data transfer to the CAC through the local cyberspace administration at the provincial level:

- where a data processor provides critical data abroad;
- where a key information infrastructure operator or a data processor processing the personal information of more than one million individuals provides personal information abroad;
- where a data processor has provided personal information of 100,000 individuals or sensitive personal information of 10,000 individuals in total abroad since 1 January of the previous year; and
- in other circumstances prescribed by the CAC for which declaration for security assessment for outbound data transfers is required.

According to the security assessment result, the CAC may rule the data provider to terminate the data export.

On 22 March 2024, the CAC issued the Regulations on Promoting and Regulating Cross-Border Data Flows. These regulations expanded the situations in which exemptions from the three data export methods mentioned above apply. They also clarified and simplified the procedures, processes, and documentations for submitting security assessments and filing standard contracts, thereby improving the framework in facilitating cross-border data flows, which is believed to bring convenience to the many foreign-invested enterprises operating in China with massive data produced.

The Network Data Security Management Regulations provide the first nationwide operational framework for important data governance and the Network Data Security Risk Assessment Measures further requires important data processors to conduct annual risk assessments, with general data processors encouraged to conduct assessments at least every three years.

The Cybersecurity Label Management Measures establish a three-tier cybersecurity labelling system (basic/enhanced/leading) for internet-connected products, helping consumers identify products with stronger security capabilities.

Law stated - 15 August 2026

Sale of data to third parties

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

In accordance with article 10 of the PIPL, no organisation or individual may illegally buy or sell the personal information of others.

Under certain specific circumstances, personal information may be shared or transferred, in accordance with applicable laws. If a processor of personal information provides personal information processed by it to other processors of personal information, it shall inform the individual of the name or names of the recipients, their contact information, the purpose of the processing, the method of processing, and the type of personal information, and obtain the individual's separate consent.

In the event of a merger, separation, dissolution, bankruptcy declaration, etc., if personal information needs to be transferred, the individual will be notified of the receiving party's name or name and contact details. The receiving party must still fulfil their obligations as a processor of personal information, which includes maintaining data security and processing it according to the original purpose. If there is a need to change how the information is processed, consent from the individual must be obtained again.

[Shanghai Data Regulation](#) expressly indicates that natural persons, legal persons and other organisations may conduct data trading in compliance with the laws and regulations. Pudong New District has set up a data exchange for the convenience of data trading, and transactions are encouraged to be secured there.

However, with regard to the circulation of personal data, the consent of individuals should be obtained or anonymised in accordance with the law and regulations, and the consent of individuals should not be obtained by means of coercion, fraud or misinformation. Engaging

in illegal trading of personal information will lead to severe legal consequences, such as administrative penalties, civil liability, and criminal charges.

With the Regulation on Network Data Security Management coming into effect and the amended Cybersecurity Law, regulatory authorities are adopting a stance of intensifying penalties for violations. Administrative penalties are categorised into different tiers based on the nature of the violation, the degree of intentional wrongdoing, and the severity of consequences, with variations in the types, scope, and severity of penalties applied accordingly. The Data Property Rights Registration Work Guidelines (Trial) establishes a unified national data property rights registration system, providing a basis for proving data ownership in transactions.

Law stated - 15 August 2026

Consumer redress

38 | 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?

The right to personal information mainly includes the following subsidiary rights:

1. The privacy disposition right: the right of a person to directly control and dominate his or her personal data. The person also has the right to decide whether, and in what manner, purpose and scope, his or her personal data will be collected, processed and used.
2. The privacy secrecy right: the right of a person to request that information be kept confidential by the information processing subject.
3. The inquire right: the right of a person to enquire about his or her personal information and the processing thereof, and to request a response. The control of information must begin with knowing what personal information is collected, processed and used, and whether the information is kept complete, correct and up to date in the process.
4. The correct or supplement right: the right to request the subject of information processing to correct and add to personal information that is incorrect, incomplete or, from time to time, new.
5. The deletion right: the right to request the information processing subject to delete personal information for legal or agreed reasons.

The protection of personal information is applicable to the activities of processing the personal information of natural persons in China and applies to the principle of territoriality, without distinguishing by nationality. Moreover, GB/T 46901-2025 (Data Security Technology – Requirements for Personal Information Transfer Based on Individual Requests) provides detailed rules on the scope, prerequisites, and procedures for personal information transfer requests.

Law stated - 15 August 2026

Non-personal data

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

In China, there is no specific law that regulates the use of non-personal data. The flow of data from China to other jurisdictions should be approved by the relevant authorities if the data reach the threshold specified by article 4 of [the Security Assessment Measures for Outbound Data Transfers](#), which doesn't distinguish between personal data and non-personal data.

Under the [CAC Regulations on Promoting Cross Border Data Flow](#) 2024, any data (personal or not) that is not 'important' is exempt from CAC security assessments, standard contract filing, or personal data certification if it meets exemption criteria (eg, generated during cross-border trade, academic cooperation, logistics). If a dataset contains neither personal information nor important data, it may be shipped offshore freely—even crossing zones—without regulatory pre approval, subject to free trade zone 'negative lists'. If the dataset is flagged as important, any unapproved export triggers a security assessment by CAC, required regardless of whether it contains personal data.

There may also have industrial specific requirements or restrictions on the processing of industrial data which may include non-personal data such as Important Data referring to the data of a specific field, a specific group or a specific region or with a certain accuracy and scale, which, once tampered with, destroyed, leaked or illegally obtained or illegally used, may directly endanger national security, economic operation, social stability, public health and security; and Core Data refer to the important data with high coverage or high accuracy, a relatively large scale and a certain depth for fields, groups or regions, which, once illegally used or shared, may directly affect political security as defined and stipulated in Administrative Measures of the People's Bank of China for Data Security in Business Fields published on 1 May 2025, which regulates the security supervision and administration of the processing activities relating to the network data generated and collected in the business fields of the PBC not involving State secrets.

Law stated - 15 August 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

China encourages and supports the digitisation of archives. The general law governing document retention, [the Archival Law](#), does not require any particular document or record types to be kept in original paper form and not converted solely to a digital representation. Instead, it emphasises that electronic archives and archives carried in traditional forms have the same legal effect, and in the case of digitised archives, the original archives shall be properly kept.

However, in several key areas digital only archiving is permitted only under strict, accredited systems—otherwise paper records must be kept just as a 'fallback' or submitted to authorities in original form. For example, under the [Notice on Regulating the Filing of Electronic Accounting Vouchers for Reimbursement 2020](#), legally issued electronic invoices or accounting vouchers can be treated as original and stored digitally only if they are verified as genuine, securely archived, and fully retrievable with audit trails; mere scanned printouts do not qualify, so paper versions or hybrid physical+digital backup must be retained if the standards aren't met.

Law stated - 15 August 2026

Retention

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

The National Archives Administration of China formulates regulations for different authority systems, stipulating minimum retention periods or permanent retention for different types of documents.

For example, the National Archives Administration of China and the Supreme People's Court collaboratively promulgated the Measures for the Administration of Litigation Archives of the People's Courts in 2013, which stipulate three retention periods: at least 20 years, at least 60 years and permanent retention. Those litigation archives with long-term value for investigation and utilisation shall be classified as permanent retention, such as those pertaining to cases with a death sentence. Those litigation archives with relatively long-term value for investigation and utilisation shall be classified to be kept for at least 60 years, such as those pertaining to cases with fixed-term imprisonment sentences of five to 15 years. Those litigation archives with short-term value for investigation and utilisation shall be classified to be kept for at least 20 years, such as those pertaining to cases with fixed-term imprisonment sentences of less than five years.

For financial institutions, the clients' identity materials shall be preserved for at least five years after the end of a business relationship or a one-time transaction; and the transaction records shall be preserved for at least five years after the completion of a transaction as stated in the Administrative Measures for Client Due Diligence and Preservation of Clients' Identity Information and Transaction Records by Financial Institutions.

Law stated - 15 August 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

E-commerce business operators

In accordance with the E-Commerce Law, the E-commerce business operators shall:

- collect and use the personal information of their users compliant with the provisions of laws and administrative regulations on the protection of personal information;
- adopt technical measures and other requisite measures to ensure the secure and stable operation of their network, prevent cybercrimes, deal with cybersecurity incidents effectively, and ensure the security of e-commerce transactions; and
- formulate cybersecurity incident emergency plans, and forthwith trigger the emergency plans upon the occurrence of a cybersecurity incident, adopt the corresponding remedial measures, and report to the relevant competent authorities.

Internet service providers

The Cybersecurity Law amended provides more requirements for internet service providers (ISPs) to ensure the security of internet transactions. ISPs must:

1. provide network products and services satisfying the mandatory requirements in the applicable national standards;
2. not install malware;
3. immediately take remedial action against any risk such as security defects or bugs that are found, inform users of the risk and report the case to the competent authority;
4. provide consistent security maintenance for the ISP's products or services;
5. expressly notify and obtain the consent of users if the products or services provided by the ISP collect user information; and
6. comply with provisions of the Cybersecurity Law as well as the relevant laws and administrative regulations governing the protection of personal information if the personal information of users is involved.

Network operators must develop an emergency plan for cybersecurity events to promptly respond to security risks such as system bugs, computer viruses, network attacks and network intrusions. For an event that threatens cybersecurity, the operator concerned must initiate the emergency plan, take corresponding remedial actions and report the event as required to the competent authority.

Network operators shall take technical and other necessary measures to ensure the security of the personal information that it collects, and to protect such information from disclosure, damage or loss. In cases of disclosure, damage or loss (or possible disclosure, damage or loss) of such information, the network operator shall take immediate remedial action, notify users in accordance with the relevant provisions and report to the competent authority.

Network operators shall strengthen the management of the information released by their users. If the operator finds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information and take measures such as deletion to prevent the dissemination of such information. The operator shall also keep a relevant record and report the case to the competent authority.

Encryption is not a mandatory security measure.

Commonly used cybersecurity standards are stipulated in the Cybersecurity Law (CSL) and the Personal Information Protection Law (PIPL), including but not limited to:

- Transparency.
- Legality for processing.
- Limitation of purpose.
- Data minimisation.
- Proportionality.
- Retention period.
- Data quality and accuracy.

Regarding transparency, the CSL mandates that network operators shall disclose the rules for collecting and using personal information, clearly stating the purposes, methods, and scope of such activities. This principle is also reflected in the Personal Information Protection Law (PIPL), which requires, under article 7, that personal information processing follows principles of openness and transparency, with explicit disclosure of the purpose, method, and scope.

Regarding legality for processing, the CSL and the Civil Code require network operators to adhere to the principles of legality, justification, and necessity when collecting and using personal information. The PIPL similarly mandates that personal information processing must be lawful, legitimate, necessary, and conducted with integrity, prohibiting misleading, fraudulent, or coercive practices.

Regarding purposes, the CSL stipulates that network operators must not collect personal information unrelated to the services they provide. PIPL also requires that the processing of personal information must have a clear and reasonable purpose, directly related to the processing activities.

Data minimisation refers to the rule that personal information processing should be conducted in a way that minimally impacts individual rights, limited to what is necessary to achieve the processing purpose, and prohibits excessive data collection in accordance with the PIPL. While the CSL and PIPL do not explicitly mention a proportionality principle, the data minimisation principle in PIPL is essentially similar, emphasising that personal information should only be processed within an appropriate and necessary scope, and in a way that minimises the impact on individual rights.

Regarding retention period, according to article 19 of the PIPL, unless otherwise stipulated by law or administrative regulations, the retention period for personal information should be as short as possible to achieve the processing purpose.

As for data quality and accuracy, article 8 of the PIPL requires that the quality of personal information shall be ensured during processing to avoid negative impacts on individual rights due to inaccurate or incomplete information.

Law stated - 15 August 2026

Data breach notification

- 43** | 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?

Both the Cybersecurity Law and the PIPL regulate that, in the case of a data breach, the network operator (ie, the information processor) shall be obliged to take immediate remedial actions, notify the users and report to a competent authority.

Under the National Cybersecurity Incident Reporting Management Measures, incidents classified as "relatively major" or above must be reported through the national 12387 platform or hotline within strict deadlines: critical information infrastructure operators within one hour, central government entities within two hours, and all other operators within four hours (with major or material incidents escalated within 30 minutes to one hour). Affected individuals must be notified without undue delay where personal information is breached, unless effective remedial measures eliminate the risk of harm. Industry-specific regulators may impose additional or shorter reporting obligations (eg, financial regulators often require one hour reporting). A final post incident summary report must be submitted within 30 days of containment. Penalties apply for delay, omission, false reporting, or concealment, while timely reporting with effective mitigation may lead to lighter or no punishment.

However, there is no detailed data breach notification system specific to e-commerce that is regulated by laws and regulations.

Law stated - 15 August 2026

Government interception

- 44** | 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?

There is no specific rule on whether authorities can require private keys to be made available. However, according to article 31 of the Cryptography Law, cryptography administrations, related authorities and the staff thereof shall not require commercial cryptography-related agencies and commercial cryptography testing or certification agencies to disclose their source codes or other proprietary cryptography-related information.

Certification authorities are permitted and operate under a licensing system. Certification authorities can only provide service after going through the approval of the Ministry

of Industry and Information Technology (MIIT) and the Ministry of Commerce. For the provision of an electronic authentication service without a licence, MIIT will order the providers to stop the illegal act and illegal income (if any) shall be confiscated.

Encrypted communications are mainly regulated under the Electronic Signatures Law, the Cryptography Law and the Administrative Measures on Electronic Certification Services.

Law stated - 15 August 2026

GAMING

Legality and regulation

- 45** | 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?

The Chinese mainland is staunchly opposed to gambling. Both online and offline gambling are illegal, with both being punishable by criminal penalties and detention.

Law stated - 15 August 2026

Cross-border gaming

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

Online betting is illegal in China. Advertising and providing access to online betting with earnings of not less than 20,000 yuan constitute a joint offence with the crime of running a casino.

As for operation of a gaming business in another jurisdiction, PRC laws require the operator to obtain authorisation from the copyright owner, and approval from competent copyright administrative departments and provincial publication bureaus. Unapproved advertisement or access services will be curbed, the operator's internet service will be stopped and its website shut down. Operation without legal authorisation from the game's copyright owner will be investigated by the National Copyright Administration. Serious infringement of copyright may constitute a criminal offence.

Regarding gaming businesses on the metaverse, clarifying legislation is yet to come. However, since the metaverse is closely intertwined with virtual currency, whose legitimacy has been denied by existing regulation, metaverse gaming in China faces considerable difficulties. Operations relevant to virtual currency could constitute the criminal offences of, for example, fund-raising fraud or illegally engaging in fund payment and settlement business.

Law stated - 15 August 2026

OUTSOURCING

Key legal issues

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

Agreement

When choosing the provision of services on an outsourced basis, an enterprise shall try to avoid direct personnel management, including signing any written agreement with outsourced employees or paying salaries and social insurance premiums. Instead, the enterprise should sign standardised outsourcing agreements with its outsourced services provider.

Qualification

The outsourced services provider shall possess corresponding qualifications if the outsourcing business involves qualification requirements.

Business secrets

Enterprises shall not assign outsourced employees to core positions that may have access to the business secrets of the enterprise.

Tax

If an outsourced service provider is qualified for the recognition of advanced technology-based service enterprises in terms of employee qualifications, sources and percentages of revenue, it will be entitled to tax incentives.

Law stated - 15 August 2026

Sector-specific issues

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

In general, outsourcing of digital business services is allowed and encouraged. A few particular digital financial services are prohibited from outsourcing, such as the following:

1. Risk management of commercial banks accepting loaning applications online. According to the rule, commercial banks must strengthen their responsibilities regarding risk control. Banks shall independently carry out risk management of loans operated through internet platforms, and complete the whole risk management process, which has important impacts on loaning risk assessment and risk control. It is strictly prohibited to outsource the key links of loaning management at any time, including pre-loan, in-loan and post-loan.

2. Information technology of banks, asset management companies and insurance institutions, which is related to the financial institution's core competitiveness, shall not be outsourced.

Additionally, the Regulation on Risk Supervision of Information Technology Outsourcing in Banking and Insurance Institutions establishes specific rules for IT outsourcing. The regulation creates a unified IT outsourcing management system, with a core focus on identifying, assessing, monitoring, and controlling risks throughout the outsourcing lifecycle.

Law stated - 15 August 2026

Contractual terms

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

It is provided in the Measures for the Risk Supervision of Information Technology Outsourcing of Banking and Insurance Institutions that the following contents in information technology outsourcing contracts shall be specified, including but not limited to:

- Service scope, service content, service requirements, working time limit and arrangement, responsibility allocation, delivery requirements, relevant restrictions in follow-up cooperation, and agreement on service quality assessment and evaluation.
- Compliance management, internal control and risk management, compliance with laws and regulations and internal management systems of banking and insurance institutions, and notification and implementation mechanism for regulatory policies.
- Service continuity requirements where the sustained service as a management requirement of the provider must align with the business requirements of continuity of banking and insurance institutions.
- The right of banking and insurance institutions to conduct risk assessment, monitoring, inspection and auditing of service providers, and service providers undertake to accept the supervision and inspection of the outsourcing services of banking and insurance institutions undertaken by the China Banking and Insurance Regulatory Commission.
- Triggering conditions for contract modification or termination, and transitional arrangements for contract modification or termination.
- The ownership of relevant information and intellectual property rights in outsourcing activities, as well as the content and scope that service providers are allowed to use, and the requirements for service providers to use legal software and hardware products.
- Resource support clauses.
- Confidentiality and consumer rights protection clauses where the information of the banking and insurance institutions shall not be used or disclosed unless permitted

by the contract and the data incurred shall not be transferred, appropriated or be utilised for interests otherwise agreed upon other than in the contract.

- Dispute resolution mechanism, breach of contract and compensation clauses where cross-border outsourcing should specify the applicable law and jurisdiction for dispute resolution. In principle, Chinese arbitration institutions and Chinese courts should be selected for jurisdiction, and Chinese laws should be applied to resolve disputes.
- Reporting terms, including at least the content and frequency of regular reports, reporting routes, reporting methods and time-limit requirements in case of emergencies.

What is more, the banking and insurance institutions shall expressly require in the contract or agreement that service providers shall not subcontract outsourced services including in disguised form. When it comes to subcontracting outsourced services, the contract or agreement shall include the following terms:

- it is not allowed to subcontract the main business of outsourcing services;
- the main service provider is generally responsible for the service level and ensures that the subcontracted service providers can strictly abide by the outsourcing contract or agreement; and
- the main service provider monitors the subcontracting service providers and fulfils the obligation of notification or report approval for changes of subcontracting service providers.

Law stated - 15 August 2026

Employee rights

- 50** | 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 speaking, in the company, the benefits related to salary, annual leave and promotion of outsourced employees might be inferior to regular employees. In terms of the rights of employees (such as severance or consultation) under Chinese employment law, there is no legal distinction between outsourced and regular employees.

Law stated - 15 August 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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 2017, the State Council of China issued the [New Generation Artificial Intelligence Development Plan](#) (the Plan), providing administrative guidance for artificial intelligence (AI) from the perspective of industrial policy promotion, support and development. Following the Plan, the National New Generation Artificial Intelligence Governance Professional Committee was established, which has issued [the Governance Principles for New Generation Artificial Intelligence – Developing Responsible Artificial Intelligence \(2019\)](#) and [the Ethics Norms for New Generation Artificial Intelligence \(2021\)](#).

In accordance with the Ethics Norms, suppliers are recommended to conduct quality monitoring and use evaluation of AI products and services to avoid undue harm. In 2023, the CAC and other government ministries jointly issued the [Interim Measures for the Management of Generative Artificial Intelligence Services](#), which is the first supervisory regulation in China regarding artificial intelligence. The State Council's 2024 Legislative Work Plan states that a draft of the Artificial Intelligence Law is scheduled to be submitted to the National People's Congress Standing Committee for review.

On 7 March 2025, the CAC and other government ministries jointly issued the [Artificial Intelligence Generating Synthetic Content Labelling Methods](#) (effective from 1 September 2025), to regulate the labelling of artificial intelligence generating synthetic content. The accompanying mandatory national standard GB 45438-2025 (Cybersecurity Technology – AI-Generated Content Identification Methods) will synchronously take effect.

Since then, China's AI regulatory framework has expanded significantly:

- The Measures for the Management of Anthropomorphic AI Interactive Services (2026), jointly issued by five departments, impose specific requirements including: no virtual intimate relationship services for minors; anti-addiction mechanisms (2-hour usage reminders); extreme emotion identification and intervention functions; and mandatory safety assessments for services with over 1 million registered users or 100,000 monthly active users.
- The AI Technology Ethics Review and Service Measures (Trial) (2026), jointly issued by ten departments, establish ethics committees (or service centres) as implementation entities, with general/simplified/emergency procedures, and a list of activities requiring expert review covering: (1) human-machine fusion systems with strong influence on human behaviour, psychology, and life/health; (2) algorithm models, applications, and systems with public opinion mobilisation capabilities; and (3) highly autonomous automated decision-making systems for safety-critical scenarios.
- The Opinions on the Standardized Application and Innovative Development of Intelligent Agents (2026), establish a classified and graded governance framework for AI agents, requiring clear decision-making authority boundaries, behaviour controls, and supply chain security measures.
- The Digital Virtual Human Information Service Management Measures (draft for comment) require “digital human” labels to be displayed throughout the service and prohibit virtual intimate relationship services for minors.
-

The Internet Information Service Management Measures (revised draft for comment) add a dedicated “Intelligent Information Services” chapter, requiring AI training data to have legal sources, mandatory AI-generated content labelling, algorithm recommendation governance, and agent service security management.

- GB/Z 185-2026 (Artificial Intelligence – Agent Interconnection) series (7 standards, effective 22 May 2026) provides technical specifications for agent identity codes, identity management, agent description, discovery, interaction, and tool invocation.
- The Cybersecurity Standard Practice Guide – Security Guidelines for Agent Deployment and Use (2026) covers security guidance across five stages: assessment, preparation, deployment, use, and decommissioning.

On the basis of the above rules, the following requirements are imposed for use of AI:

- The AI developers shall:
 - strengthen self-discipline in all aspects of technology research and development;
 - improve data integrity, timeliness, consistency, standardisation and accuracy;
 - improve transparency and reliability in algorithm design, implementation and application;
 - avoid possible data and algorithm biases in data collection; and
 - conduct science and technology ethics review for AI activities that may pose ethical risks, with expert review mandatory for high-risk activities including human-machine fusion systems, algorithms with public opinion mobilisation capabilities, and highly autonomous decision-making systems in safety-critical scenarios.
- The AI suppliers shall:
 - abide by rules on market access and competition, and avoid infringement of intellectual property (IP) rights;
 - strengthen the quality monitoring and use evaluation;
 - add explicit + implicit labels to all AI-generated outputs;
 - inform users of the functions and limitations of AI products and services, and protect users’ right to know and consent;
 - respond to and process user feedback in a timely manner, and formulate emergency mechanisms and loss compensation plans or measures;
 - for anthropomorphic interactive AI services, implement anti-addiction mechanisms (2-hour usage reminders), deploy extreme emotion identification and intervention functions, and provide prominent AI identity labelling;
 - for financial sector AI applications, ensure board-level governance oversight, conduct risk classification, and strictly prohibit using customers’ personal information (names, ID numbers, phone numbers, bank card numbers) for generative AI training; and

- for AI services with public opinion attributes or social mobilisation capabilities, complete algorithm filing, security assessment, and, for generative AI services, large model filing.
- The AI users shall:
 - use in good faith;
 - avoid improper use and abuse of AI products and services, and avoid unintentional damage to the legitimate rights and interests of others;
 - label AI-generated content when uploading to platforms;
 - not use AI products and services that do not comply with laws, regulations, ethics and standards, and prohibit the use of AI products and services to engage in illegal activities;
 - provide timely and proactive feedback on issues such as technical security loopholes, policy and regulation vacuums, and regulatory lag found in use; and
 - improve usability to ensure safety and efficient use of AI products and services.

Law stated - 15 August 2026

IP rights

- 52** | 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?

The Interim Measures for the Management of Generative Artificial Intelligence Services issued in 2023 states that when providers of generative artificial intelligence services conduct pre-training, optimisation training, or other data processing activities, they must not infringe on the intellectual property rights legally held by others. Currently, there are no specific rules concerning IP and AI or machine learning. Therefore, such issues are still under general regulation of IP laws, such as the [Copyright Law](#), Trademark Law and [Patent Law](#).

In practice, the protection by IP rights for AI or machine learning remains controversial.

Under the Patent Law

Article 25 of the Patent Law stipulates that 'scientific discoveries, rules and methods of intellectual activities, etc shall not be granted patent rights'. In the field of AI, the innovation of algorithms is the core of every invention and creation at the technical level. Whether pure algorithms belong to 'the rules and methods of intellectual activities', and whether they can be patented, is controversial. The Announcement stipulates that if a claim contains technical features in addition to algorithmic features or features of business rules and

methods, then the claim, as a whole, is not rules and methods for mental activities, and shall not be excluded from patentability. Whether the provision will further help AI be protected under the Patent Law is unclear.

Under the Copyright Law

Products generated by AI without human participation, based on current laws, cannot be regarded as works protected by the Copyright Law.

Under the Anti-Unfair Competition Law

Commercial secrets refer to technical information, business information and other commercial information that is not known to the public, has commercial value and has been kept secret by the obligee. Therefore, as the core of AI enterprises, algorithms also have great commercial value, and enterprises usually take strict confidentiality measures to keep the algorithms secret. [The Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases of Infringement of Trade Secrets](#) also clarifies that the people's courts can protect algorithms as trade secrets. Therefore, AI might be protected in this way.

China has no special laws or regulations on the ownership of IP created by AI or machine learning systems. However, in a judgment rendered in 2020, Nanshan Primary People's Court, Shenzhen, Guangdong recognised that the works generated by Dreamwriter, an AI robot developed by Tencent, constituted works protected by the Copyright Law, and Tencent, as a legal entity, owned such copyrights. This precedent became one of the 'Top 10 Cases in 2020' certified by the Supreme People's Court, which indicates its value as guidance concerning such ownership.

Law stated - 15 August 2026

Ethics

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

The 2019 AI Governance Principles outline eight governance pillars—fairness, justice, transparency, accountability, privacy, inclusivity, security, cooperation—explicitly stating the need to eliminate bias in data, design, and deployment.

[The Ethics Norms for New Generation Artificial Intelligence](#), issued by China's national AI governance committee, applies throughout the full AI life-cycle—management, R&D, supply, and use—with explicit guidance to avoid biases in data and algorithms and encourage transparent, accountable governance.

The Interim Provisional Measures for the Management Administration of Generative Artificial Intelligence Services stipulate that when providing and utilising generative AI (GAI) services, the laws and regulations shall be complied with, as well as social moral principles and ethics, which include:

1. Conforming to socialistic core values, and not generating content that incites subversion of the state power or the overthrow of the socialistic system, endangers national security and interests, damages the national image, incites separatism, undermines national unity and social stability, propagates terrorism, extremism, ethnic hatred and discrimination, violence, pornography, and false and harmful information.
2. Taking effective measures to prevent discrimination in terms of nationality, religion, country, region, gender, occupation, health, etc, in the process of algorithm design, training data selection, model generation and optimisation, service provision, etc.
3. Respecting intellectual property rights and commercial ethics, protecting trade secrets, and not committing acts of monopoly and unfair competition with the advantages of algorithms, data, and platforms.
4. Respecting the legitimate rights and interests of others, not endangering others' physical and mental health, and not infringing upon others' rights of portrait, reputation, honour, privacy or personal information.
5. Taking effective measures in light of the characteristics of different types of services to boost the transparency of GAI services and the accuracy and reliability of content generated.

It is worth noting that both the service providers and the users are obligated to comply with the ethics. In fact, the requirements mainly concentrate on the role of GAI service providers as content producers who thus undertake duties of compliance under the Cyber Security Law and other administrative regulations.

The Opinions on Strengthening Science & Technology Ethics Governance (2022) and the Ethics Review Measures (2023) require R&D entities to set up ethics committees, conduct ethical review, and address potential algorithmic discrimination or social risks, particularly in sensitive applications and public opinion systems.

The AI Technology Ethics Review and Service Measures (Trial) (effective 20 March 2026) provide the most comprehensive ethics framework to date, requiring ethics committees (or service centres) to review AI activities based on principles including: human welfare, fairness and justice, controllability and trustworthiness, transparency and explainability, accountability and traceability, and privacy protection. The Measures set out a three tier procedure (general, simplified, emergency) and establish a list of AI activities requiring expert review. The Cybersecurity Standard Practice Guide – AI Application Ethics Security Guidelines (draft for comment) further provides practical ethical security guidance for AI applications.

Law stated - 15 August 2026

TAXATION

Online sales

- 54** | Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

In general, tax is imposed whenever a transaction takes place, whether online or offline. However, in Chinese tax law practice, virtual product transactions between individuals or between individuals and companies are exempt from value-added tax (VAT) if they do not reach the tax threshold. For individuals who cannot provide evidence of the original value of their property, the competent tax authorities shall approve the original value of their property.

For transactions between companies in China, the seller company shall pay tax in accordance with Chinese tax law. As for cross-border virtual products between companies, China's current practice is that foreign companies that provide virtual product services must set up a standing body in China or cooperate with a domestic entity in China. The authorities will impose VAT on the standing body or cooperative entity. There will also be a tax imposed on for-profit businesses from China.

Law stated - 15 August 2026

Server placement

55 | 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?

If the servers installed overseas by a domestic company are used solely for offshore websites, such servers will not be subject to taxes in China. Nevertheless, if such servers are installed abroad and still engaged in network business related to China or the offshore companies send professionals to provide technical services in China the domestic company receiving services shall withhold the taxes and surcharges.

If an offshore company placed servers in China and receives revenue from China through such servers, that portion of the revenue related to China is subject to taxes.

Where there are special agreements on tax collection of cross-border income in tax treaties or agreements signed between China and an overseas country or region, the domestic company may opt to apply the preferential tax rate in the tax treaties or agreements.

China's [VAT Law](#) (effective from 1 January, 2026) clarifies that a cross border intangible and services transaction is considered as occurring within China (ie, VAT-applied) if the service or intangible is consumed in China, or the supplier (sales side) is within China, hence will be VAT taxable. [Implementing Regulations of the VAT Law](#) elaborates that 'Consumed in China' includes:

- services or intangibles sold by a foreign supplier to a Chinese entity unless the service is entirely consumed offshore (ie, on-site abroad);
- if the service or intangible is directly related to goods, real estate, or natural resources in China, it's deemed consumed in China; or
- other additional circumstances specified by the State Council or Ministry of Finance and State Taxation Administration.

In other words, the 'consumed in China' rule applies even when the supplier is outside mainland China, especially when servicing, technology, or intangible usage happens in China, unless it's entirely consumed outside China.

Law stated - 15 August 2026

Electronic invoicing

- 56** | 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?

E-invoicing has been generally implemented in China. In 2015, China started to implement e-invoicing for VAT regular invoices, and in 2020 started to implement e-invoicing for VAT special invoices.

China implements a uniform format for e-invoicing. As of 2019, the national standard Electronic Invoice Based Information Specification came into effect, stipulating the uniform format and required information for e-invoices.

The State Administration of Taxation has built a nationwide unified e-invoice service platform. Issuance of e-invoices are synced on the platform, and thus there is no need to submit copies of e-invoices to the State Administration of Taxation.

The State Administration of Taxation issued the Decision on Amending the Detailed Rules for the Implementation of the Invoice Management Measures, which took effect on 1 March 2024. The newly revised rules supplement and improve the procedures for the issuance and use of electronic invoices. More importantly, the rules provide a clearer definition of invoice fraud.

Law stated - 15 August 2026

DISPUTE RESOLUTION

Venues

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

China has established three internet courts in Beijing, Hangzhou and Guangzhou. These courts specialise in internet-related cases online, all of which are located in the most booming and prosperous areas of China's internet industry. These internet courts are skilled in hearing disputes arising from contractual disputes over online shopping or services and underwrite financial loans, as well as online copyright disputes and internet-related public interest litigation, among others. Most of the evidence in the cases heard by internet courts is in the form of electronic data and is stored on the internet.

Law stated - 15 August 2026

ADR

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

For online or digital disputes, ADR is a very common practice in China. E-commerce platforms such as Alibaba and JD.com have set up their own ADR platforms and most consumers are accustomed to solving online shopping contractual disputes through such platforms.

For example, on Alibaba, when a consumer is dissatisfied with goods or services online, the consumer usually submits evidence and negotiates with the supplier first. After the consumer submits the dispute, the two parties have three to 30 days to negotiate without the involvement of the e-commerce platform itself. If the supplier provides a different proposal, the consumer could request Alibaba's assistance by clicking the 'escalate dispute' button or may continue to negotiate with the seller.

In general, the ADR platforms of businesses are more inclined to protect the interests of consumers.

However, some consumers will directly seek the help of the official ADR platform, which is the 12315 platform. The 12315 platform is a hotline that is directly affiliated with the State Administration for Market Regulation (SAMR). In addition, at a local level, many SAMR offices have also established their own separate complaint channels in the form of hotlines or social media accounts.

Law stated - 15 August 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

Cybersecurity Law Amendment Significantly Increases Penalties

On 28 October 2025, the Standing Committee of the National People's Congress adopted the first amendment to the Cybersecurity Law since its enactment in 2017, which took effect on 1 January 2026. The amendment introduces a tiered penalty regime, raising the maximum fine for severe violations to 10 million yuan for enterprises and 1 million yuan for directly responsible individuals. It also expressly incorporates support for AI technology R&D and security supervision into the law (article 20), and extends the territorial scope of the law to allow authorities to take action against overseas entities for any activities endangering China's cybersecurity, not only those targeting critical information infrastructure.

AI Regulatory Framework Expands Rapidly

The period from September 2025 to July 2026 saw a significant expansion of China's AI governance framework. The AI-Generated Synthetic Content Labelling Methods (effective 1 September 2025), together with mandatory national standard GB 45438-2025, require both explicit and implicit labelling of all AI-generated outputs. The AI Technology Ethics Review and Service Measures (Trial) (effective 20 March 2026), jointly issued by ten departments, establish ethics committees as implementation entities, with a three tier procedure (general, simplified, emergency) and a list of high risk AI activities requiring expert review. The Measures for the Management of Anthropomorphic AI Interactive Services (effective 15 July 2026) prohibit virtual intimate relationship services for minors and mandate anti addiction mechanisms and extreme emotion identification functions. The Opinions on the Standardized Application and Innovative Development of Intelligent Agents (effective 8 May 2026) establish a classified and graded governance framework for AI agents, accompanied by the GB/Z 185-2026 (Artificial Intelligence – Agent Interconnection) series of seven national standards (effective 22 May 2026) providing technical specifications for agent identity codes, management, discovery, interaction, and tool invocation. The Cybersecurity Standard Practice Guide – Security Guidelines for Agent Deployment and Use (effective 1 July 2026) further provides practical security guidance across five lifecycle stages.

Cross-Border Data Transfer Regime Completed

The cross border personal information transfer compliance framework was finalised with the adoption of the Measures for Certification of Cross Border Personal Information Transfer (effective 1 January 2026), completing the “three pillars” of data export compliance alongside security assessment and standard contracts. GB/T 46068-2025 (Data Security Technology – Security Certification Requirements for Cross border Personal Information Processing Activities) (effective 1 March 2026) serves as the core certification standard. The Network Data Security Risk Assessment Measures (effective 20 August 2026) require important data processors to conduct annual risk assessments, with general data processors encouraged to conduct assessments at least every three years. The Regulations on Promoting and Regulating Cross Border Data Flows expanded exemption scenarios and clarified procedures for security assessments and standard contract filings.

Personal Information Protection Deepens with New Standards and Audits

The GB/T 46903-2025 (Data Security Technology – Personal Information Protection Compliance Audit Requirements) (effective 1 July 2026) provides detailed audit requirements, including a three tier auditor classification and frequency requirements for processors handling different volumes of personal information. GB/T 46901-2025 (Data Security Technology – Requirements for Personal Information Transfer Based on Individual Requests) (effective 1 July 2026) establishes detailed rules on the scope, prerequisites, and procedures for personal information transfer requests. The Large Network Platform Personal Information Protection Regulations (draft for comment) propose strict DPO requirements, including Chinese nationality, no permanent residency abroad, and veto power over personal information processing matters. The Provisions on Simplified Personal

Information Protection Measures for Small Personal Information Processors which will take effect on 1 September 2026 define small processors as those handling fewer than 100,000 individuals' personal information, officially implementing simplified compliance pathways for qualifying entities.

Platform Economy Faces Tighter Regulation and Competition Rules

The Anti Unfair Competition Law amendment (effective 15 October 2025) introduced substantial new provisions targeting digital platforms, including prohibitions on forcing merchants to sell below cost and restrictions on using data and algorithms for unfair competition. The Internet Platform Price Behavior Rules (effective 10 April 2026) regulate dynamic pricing and prohibit price discrimination based on consumer profiles, requiring clear disclosure of pricing rules. The Internet Platform Anti Monopoly Compliance Guidelines (effective 28 January 2026) provide detailed guidance on monopoly agreements, abuse of market dominance, and concentration. The Live Streaming E-commerce Supervision and Management Measures and the Rules on the Supervision and Management of Online Transactions Platform, both adopted in 2026, establish clear responsibilities for live streamers and platforms and regulate platform rule making and enforcement.

Minor Protection Online Receives Specialised Attention

The Classification Measures for Network Information Potential to Affect Minors' Physical and Mental Health (effective 1 March 2026), jointly issued by eight departments, define four categories of "adverse information" and require prominent warnings before display, with prohibitions on presenting such information in key sections. The Identification Measures for Network Platform Service Providers with Large Numbers of Minor Users establish both quantitative and qualitative criteria for identifying platforms with significant minor user impact, triggering enhanced compliance obligations.

Data Elements and Digital Infrastructure Gain New Policy Frameworks

The Data Property Rights Registration Work Guidelines (Trial) (effective 1 July 2026) establish a unified national data property rights registration system with a "three rights separation" structure (holding rights, usage rights, and operation rights). The National Cybersecurity Incident Reporting Management Measures (effective 1 November 2025) establish mandatory reporting timelines for cybersecurity incidents, with critical information infrastructure operators required to report within one hour and other operators within four hours. The Cybersecurity Label Management Measures (effective 1 July 2026) introduce a three tier cybersecurity labelling system for internet connected products. The Provisions on Promoting and Standardizing the Application of Electronic Documents (effective 1 September 2026) encourage the use of electronic documents in trade and logistics, while the Measures for the Administration of Short Message Services (2026 Revision) (effective 1 May 2026) establish "express consent" as the baseline for commercial SMS, prohibiting mixed use of port codes and requiring sender identity verification.

Major Overhaul of E-Commerce Law Proposed to Target Platform Giants



On 4 July 2026, the State Administration for Market Regulation (SAMR) and the Ministry of Commerce released a sweeping Draft Amendment to the E-Commerce Law for public consultation. Moving beyond traditional e-commerce definitions, the amendment expands its regulatory scope to all platform economy participants including digital services, ride-hailing, and livestreaming networks. Crucially, the draft introduces severe turnover-based liabilities of up to 5 per cent of an enterprise's prior year revenue besides rigid fixed-sum fine caps for serious anti-competitive behaviours. Additionally, reflecting heightened geopolitical awareness, the draft introduces legal mechanisms allowing Chinese digital businesses to implement lawful countermeasures against foreign trade restrictions or sanctions, significantly reshaping the cross-border digital commerce risk landscape.

Law stated - 15 August 2026



Jan Holthuis
Yongmei Evers Cai

j.holthuis@burenlegal.com
y.cai@burenlegal.com

BUREN

[Read more from this firm on Lexology](#)

Germany

[Franziska Ladiges](#), [Matthias Orthwein](#), [Stefan Peintinger](#), [Johannes Schäufele](#), [Daniel Meßmer](#)
[SKW Schwarz](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The German government continues to place a strong focus on digitalisation. This trend is largely shaped by developments at the EU level, where the Digital Decade – a political agenda aiming for Europe's digital transformation by 2030 – has introduced numerous legislative proposals across various sectors. The EU and Germany are focused on establishing a reliable, harmonised and trustworthy legal framework for the digital age in Europe, hoping to create a competitive advantage for European companies. However, whether this advantage will materialise remains to be seen. In contrast, many stakeholders believe that the high density of regulations could potentially stifle growth and innovation. The EU has thus begun to further align the various legislative measures and paddled back on some perceived overregulation.

Law stated - 1 January 2025

Legislation

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

The legal landscape in the areas mentioned has undergone substantial legislative reforms in recent years. Many sectors are no longer governed solely by national law but are now subject to EU-wide regulation and/or a combination of both.

Foremost among these developments is the Digital Services Act (DSA), which has been fully applicable across the EU since February 2024. The DSA primarily regulates online platforms and search engines, introducing rules on content moderation, notice-and-action procedures, terms of service, advertising transparency, and numerous other compliance obligations. For particularly large platforms - often referred to as gatekeepers - the Digital Markets Act (DMA) also applies, establishing additional obligations to ensure fair competition in digital markets. Furthermore, the EU introduced a substantial AI regulation with the EU AI Act, that governs the development, introduction and use of AI Systems from a risk based approach within the EU.

The increasing cyber risks in the EU are met with two further legislative acts: DORA and CRA. The [Digital Operational Resilience Act \(DORA\)](#) is a regulation introduced by the European Union to strengthen the digital resilience of financial entities. It ensures that banks, insurance companies, investment firms and other financial entities can withstand, respond to, and recover from ICT (Information and Communication Technology) disruptions, such as cyberattacks or system failures. The [Cyber Resilience Act \(CRA\)](#) aims to safeguard consumers and businesses buying software or hardware products with digital elements. The CRA addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates. It also tackles the challenges consumers and

businesses currently face when trying to determining which products are cybersecure and in setting them up securely, making it easier to identify hardware and software with the proper cybersecurity features.

At the national level, important legislation includes the German Telecommunications Act (TKG), which was recently reformed to extend its scope to cover over-the-top (OTT) services.

The German State Media Treaty (MStV) governs the activities of a wide range of media platforms. The Network Enforcement Act (NetzDG), which applies specifically to social media platforms, remains the subject of ongoing debate. Its scope of application has been significantly curtailed with the entry into force of the DSA, and it now applies only supplementarily, to the extent that it does not conflict with or is not superseded by EU law.

With regard to the processing of personal data, the General Data Protection Regulation (GDPR) provides the overarching legal framework at EU level. In addition, the German Federal Data Protection Act (BDSG) and the Telecommunications-Telemedia Data Protection Act (TDDDG) are relevant. The latter governs, for example, the placement of cookies in web browsers and the access to or reading of data, including non-personal data, from end-user devices.

For marketing and digital business activities, the Act Against Unfair Commercial Practices (UWG) is of particular importance. Consumer protection law and various sector-specific regulations - for example in the fields of financial services, insurance, and product distribution - are also essential sources of law for businesses operating in the digital economy.

With the so called Omnibus Directive, the EU now harmonised and aligned many of the different compliance obligations of the above outlined legislative actions as well as lessened some of the burdens of compliance for SME within the Union.

Law stated - 1 January 2025

Regulatory bodies

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

There are no authorities or public administrative bodies specifically mandated to regulate e-commerce as a distinct sector. Instead, regulatory oversight is exercised by authorities responsible for particular areas of law, which take enforcement action against unlawful conduct within their respective mandates. These include, most notably, the Federal Media Authorities, The Federal Data Protection Authority as well as the Data Protection Authorities at the state level, the Federal Ministry of Justice and Consumer Protection - which is responsible for the NetzDG - and the Federal Network Agency (BNetzA), which oversees telecommunications and access tariffs.

With the introduction of the DSA, the Federal Network Agency (BNetzA) has assumed its role as the central Digital Services Coordinator in Germany. In this capacity, the agency is responsible for monitoring compliance with the new rules applicable to online services.

In cases of non-compliance, it has the authority to impose fines and other penalties. It has not yet been definitively decided, but it is possible that the BNetzA will also assume supervisory responsibilities in the field of artificial intelligence in Germany.

The BnetzA as well as other potential authorities are currently in talks to represent the national authority regarding the supervision of compliance with the newest AI regulation.

A significant amount of regulatory enforcement also takes place within the market itself under civil law. Privately organised bodies, such as consumer protection associations and competition watchdogs, are empowered to take action against unlawful business practices. They typically do so through cease-and-desist claims, but may also pursue claims for damages or disgorgement of profits. Such actions are brought before civil courts on the basis of specific legislation - namely, the Act on Injunctive Relief in the event of infringements of consumer protection and the UWG.

Law stated - 1 January 2025

Jurisdiction

- 4** | 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?

As a result of its ubiquity rules, the key tests are based on the EU's Rome I and Rome II Regulations, as well as Brussels I bis. The main question is typically whether a certain activity was directed at the German market or its participants, and in some cases courts additionally require a 'commercial effect.' Within the EU, this may be subject to certain, albeit limited and often sector-specific, country-of-origin principles.

Law stated - 1 January 2025

Establishing a business

- 5** | 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?

With regard to establishing a business, the rules for online businesses do not differ substantially from those applicable to brick-and-mortar enterprises. Depending on the place of establishment, a general business permit or sector-specific licenses - such as those required for offering financial services or conducting linear broadcasting activities - may be necessary. These requirements may be subject to exemptions based on the European freedom to provide services, for example, through passporting or by relying on licenses issued by other EU or EEA member states.

Law stated - 1 January 2025

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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?

The validity of electronic contracts is based on the same principles as the validity of contracts in general. A contract is formed where one party makes an offer and another party accepts this offer. Actual activity is needed to express a declaration of will to contract. Click-wrap contracts are a common standard. Crucial elements to consider regarding consumer contracts are special formal requirements for due formation – the button solution from the EU Consumer Rights Directive – and that general terms and conditions can duly be taken note of prior to the contracting process and are duly agreed to apply.

Law stated - 1 January 2025

Applicable laws

- 7 | 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?

Yes, the choice of governing law, language of the contract and forum for disputes is limited with regard to business-to-consumer contracts. Mandatory consumer information must generally be given in the German language. Choices can be made more freely in business-to-business contracts.

Law stated - 1 January 2025

Electronic signatures

- 8 | 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?

The law generally allows free form of contracting, including digital or e-signatures. However, certain types of contracts per statute require a specific form. Typically, these requirements are tied to specific types of transactions with high impact, like acquiring shares in companies or purchasing property. If the form requirement is not met, the contract is invalid.

Where statutory law requires a specific form, such as written form or notarial form, electronic contracts are typically not sufficient to form a valid contract. However, a required statutory written form can be replaced by certain electronic means as well (the qualified electronic signature according to section 126a BGB), unless not explicitly prohibited by statutory law. The technical requirements for a qualified electronic signature are set out in Regulation (EU) 910/2014 of 23 July 2014 (the eIDAS Regulation) and the Trust Service

Provider Act (VDG). Providers are qualified and licensed under the eIDAS Regulation and VDG. In 2024, the EU adopted an updated version of the legislation, widely known as eIDAS 2.0. The cornerstone of this update is the upcoming European Digital Identity (EUDI) Wallet. This personal digital wallet will allow citizens and businesses to securely store their identification data (eg, driver's licenses, professional qualifications, university degrees) and share them on-demand across the EU with both public and private sector organisations.

The same general principles apply to signing of digital information.

Law stated - 1 January 2025

Breach

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

Consumers can use consumer arbitration under the German Consumer Dispute Resolution Act (VSBG). However, participation in online dispute settlement proceedings in front of a consumer arbitration board is generally not required for businesses. There are no special remedies for the breach of electronic contracts.

Law stated - 1 January 2025

FINANCIAL SERVICES

Regulation

- 10** | 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?

The Federal Financial Supervisory Authority supervises this area. Competition protection associations may in addition seek to enforce market behaviour rules and also against unfair consumer terms, where consumer interests are affected.

Law stated - 1 January 2025

Electronic money and digital assets

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

Electronic money, digital assets or use of digital currencies is on the one hand regulated under the Directive (EU) 2015/2366 on payment services in the internal market (PSD2) rules.

Furthermore, The European Markets in Crypto-Assets Regulation (MiCAR) provides the framework for cryptoassets. The regulation includes rules for value-referenced tokens, e-money tokens and utility tokens, but not for security tokens.

Under MiCAR, various regulations are introduced, including:

- Permit requirement: issuers and providers of cryptoassets as well as providers of certain crypto-services must apply for a permit in order to carry out their activities. This creates a higher level of trust and security for investors.
- Central register: when providing cryptoasset services across borders, companies must register their activities in a central register. This will improve transparency and reduce the risks of money laundering and terrorist financing.
- Publication obligations: companies offering cryptoassets are obliged to publish certain information, such as a white paper. This creates a comprehensive and understandable information basis for potential investors.
- Market abuse protection: MiCAR also contains regulations to protect against market abuse in connection with cryptoassets. This is intended to prevent manipulation and fraudulent activities.

Law stated - 1 January 2025

Digital and crypto wallets

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

There are certain rules, in particular, around crypto depositing. Crypto depositing is defined as:

the depositing, management and safeguarding of crypto securities or private cryptographic keys used to hold, store or dispose of crypto securities for others and the safeguarding of private cryptographic keys used to hold, store or dispose of crypto securities for others to hold, store or dispose of.

Crypto depositing is deemed a financial service requiring a licence.

Mere providers of hardware or software that enable users to store their private keys themselves using self-hosted or non-custodial wallets may not be regarded as crypto depositors insofar as the providers have no intended access to the crypto values or private cryptographic keys stored with them by the user. Information obligations may also apply to crypto depositors.

Law stated - 1 January 2025

Electronic payment systems

13 |

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

Electronic payment systems are primarily regulated under the PSD2 rules. The respective implementation laws also include rules governing third-party access to digital information in bank accounts.

Law stated - 1 January 2025

Online identity

14 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?

Third parties can be used. However, certain rules apply under the German Money Laundering Act and European Transfer of Funds Regulation stating, for example, that the responsibility under the law cannot be passed on to third parties.

Law stated - 1 January 2025

DOMAIN NAMES AND URLS

Registration procedures

15 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?

Certain registries are responsible for the allocation of a second-level domain under a top-level domain. For the geographical top-level domain.de, this is DENIC. DENIC registers the domain if it meets the requirements for registration contained in the domain guidelines and is not already registered for a third party. The domain holder has a transferable right of use under the contract with DENIC. In the case of a transfer of a.de-domain, a document containing the parties, domain and price is sufficient.

It is possible to register a country-specific domain name without being a resident in the country.

There are no restrictions around the use of URLs to direct users to websites, online resources or metaverses. In exceptional cases, however, a link to another website, online resource or metaverse may be problematic if illegal content is made available on the linked website, online resource or metaverse and the company using such link adopts this content as its own, which could also be the case by implied action. This includes situations where the link is embedded in a way that users cannot distinguish between the company's own content and the linked foreign content (eg, through framing or inline linking).

Law stated - 1 January 2025

IP ownership

- 16** | 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?

In principle, domain names or URLs (ie, the term or combination of terms used in the domain name) can be subject of trademark or copyright protection under German law. However, due to the stringent requirements for a copyright-protected work, copyright protection is only conceivable in exceptional cases, if at all, while trademark protection is likely to be much more frequent in practice.

Under certain circumstances, the owner of a trademark (or a copyright, although this case is likely to be much rarer) may take action against a conflicting – identical or similar – domain. However, such an action is usually only promising if goods or services are offered on the domain which are identical or similar to the goods and services protected by the trademark. An exception only applies if the trademark has reputation in Germany or is a well-known mark. It is important to note that, as a rule, only injunctive relief can be demanded; a claim to transfer the domain exists only in exceptional cases.

Law stated - 1 January 2025

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

Advertising on the internet must comply with the Act on Unfair Commercial Practices (UWG), which regulates the market behaviour of individual companies. This Act determines that 'unacceptable nuisance' to market participant is illegal. An unacceptable nuisance is always assumed where advertising uses a medium that is suited to distance marketing and through which a consumer is persistently solicited, even if they have expressed an objection. An unacceptable nuisance is also assumed if advertising uses a medium:

- where the identity of the sender on whose behalf the communication is transmitted is concealed or kept secret;
- that violates section 6(1) of the German Digital Services Act (DGG);
- that prompts the recipient to visit a website that violates section 6(1); or
- that provides no valid address to which the recipient can send an instruction to cease sending them further messages of that nature, without incurring costs other than transmission costs pursuant to the basic rates.

This means that advertising must always be labelled as such. If AdWords, banners and pop-ups are used, they must correctly disclose their commercial character and may need to be appropriately labelled. Influencer marketing and viral marketing (eg, refer-a-friend

schemes) should not be surreptitious advertising. Electronically supported refer-a-friend schemes have been extensively restricted in recent case law.

Digital businesses must also comply with data protection laws and the DDG. This particularly applies to tracking for advertising purposes and retargeting analysis of cookies, as well as to the use of 'like' buttons or Facebook custom audiences. In principle, it is necessary to obtain the prior express consent of the users in order for the processing of data to be lawful. In addition, the consumer must always be informed about the purpose of the data processing.

In addition, the same laws apply to online advertising as to print advertising – for example, copyright, personal and publicity rights or information obligations regarding guarantees under the Civil Code, Battery Act or Electrical Act. Furthermore, the Digital Services Act imposes transparency obligations for online advertising, including clear labelling and information on targeting criteria.

Law stated - 1 January 2025

Targeted advertising and online behavioural advertising

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

According to a European Court of Justice ruling (Case C-673/17 – *Planet49*), the prior express consent of the users is required both for the use of cookies (exception: technically necessary cookies) and the use of analysis tools such as Google Analytics. The requirement of prior express consent regarding cookies, targeting with or without cookies or other tracking technologies has now also been legally implemented in Germany, namely, in section 25 of the German Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services (TDDDG).

However, the individual requirements of such consent have not yet been conclusively clarified. Particularly, the General Data Protection Regulation (GDPR) requires informed consent, which means that users must know what they are consenting to. Therefore, comprehensive information must be provided on the specific use of cookies or other analysis tools. In practice, user consent is usually obtained via 'cookie banners'.

Law stated - 1 January 2025

Misleading advertising

19 | Are there rules against misleading online advertising?

The handling of misleading online advertising is governed by the UWG. Advertising is therefore misleading if it contains untrue or other information that could be misleading about certain circumstances. Prior proof in advance confirming the advertising statement is not required. It requires proof of the correctness of the statement to be provided only in court proceedings. This, in turn, must be subject to high standards. If studies are provided

as evidence, they must be carried out and evaluated according to recognised rules and principles of scientific research.

In some cases, there are industry-specific regulations that are applicable in addition to the UWG. For example, within the framework of the Therapeutic Products Advertising Act, scientific evidence is required for advertising claims whose alleged therapeutic efficacy is disputed by experts, or for advertisers who do not have scientifically substantiated research results.

Law stated - 1 January 2025

Restrictions

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

In principle, any digital product can be offered online. However, in some cases, sector or product-specific laws must be observed. For example, media (films, photos, games, etc) that glorify violence, are pornographic or contain other content that is subject to the protection of minors may not be offered online without the appropriate permissions. Consequently, any business seeking to sell products online should ensure that the products are advertised and offered according to such sector or product-specific law.

Law stated - 1 January 2025

Direct email marketing

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

The recipient's prior express consent is required for advertising using an automated calling machine, a fax machine or email (see section 7(2) No. 3, UWG). This applies regardless of whether the recipient is a consumer or another market participant. The consent of an email recipient should be verified for the purpose of proof (double opt-in). Email marketing without consent is only permitted in an existing customer relationship, if certain conditions are met (see section 7(3), UWG). Neither the sender nor the commercial character of the message may be concealed (section 6, German Digital Services Act (DDG)). In addition, the requirements of the GDPR must be met.

Law stated - 1 January 2025

ONLINE PUBLISHING

Hosting liability

22 | 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?

The liability of providers is regulated in the German Digital Services Act (DDG). According to this, providers are only responsible for their own content (section 7(1), DDG). Hosting providers are generally not responsible for the content. It would be unreasonable to expect them to check all content. However, as soon as indications of infringements have been given, the host provider is obliged to block the infringing content and to prevent similar infringements (section 10, DDG). Website providers and other telemedia providers are fully responsible for their own content. They are also responsible for the content of third parties (eg, when using user-generated content). These providers are also liable for links to illegal content, at least at the time they become aware that the content is illegal.

Law stated - 1 January 2025

Content liability

- 23** | 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?

The liability of providers is regulated in the DDG. According to this, providers are only responsible for their own content (section 7(1), DDG). Hosting providers are generally not responsible for content – it would be unreasonable to expect them to check all content. However, as soon as indications of infringements have been given, the host provider is obliged to block the infringing content and prevent similar infringements (section 10, DDG). The online platforms or content providers are not liable if they have implemented a functioning notice and take-down procedure according to these principles. There are no prior obligations to post any notices in this regard.

Website providers and other telemedia providers are fully responsible for their own content. They are also responsible for the content of third parties (eg, when using usage-generated content). These providers are also liable for links to illegal content, at least at the time they become aware that the content is illegal.

Law stated - 1 January 2025

Shutdown and takedown

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

Providers can generally remove defamatory or infringing content without permission if it is legally established that the content is illegal, unless, for example, the content is protected by secrecy of telecommunications.

Law stated - 1 January 2025

INTELLECTUAL PROPERTY

Data and databases

25 | Are data and databases protected by IP rights?

Data and databases may be protected under German copyright law if the selection or arrangement of the individual elements constitutes a personal intellectual creation (Section 4 German Copyright Act, UrhG). A purely technical, schematic or routine selection or arrangement is not sufficient. Even a simple stringing together of data does not constitute copyright protection. Databases that do not constitute a personal intellectual creation enjoy so-called 'database producer protection' under the EU Database Directive, which is implemented in Germany via Sections 87b-f German Copyright Act.

Such protection is aimed at the investment, i.e. the capital, time and effort required to obtain, verify and present the data. It does not protect individual data, but only the database as a whole or substantial parts thereof from unauthorised extraction and reproduction. The term of protection is 15 years from the completion or publication of the database. The criteria for the protectability of such databases are (1) the existence of a collection of works, data, or other independent elements, (2) which are organised systematically or methodically and are individually accessible, (3) and in whose creation, verification, or presentation a substantial investment (in terms of time, money, or organisational resources) has been made. Typical examples include large address or customer databases, price and product databases, and scientific or technical measurement databases involving a significant effort to collect the data. The database owner may prohibit: (1) the extraction and/or reuse of a substantial part of the database's content, and (2) the systematic or repeated extraction of insubstantial parts. In practice, this means that extensive "scraping" or bulk downloads may infringe database rights even if each individual data element is not protected.

In the event of infringements, the rights holder can enforce their rights by issuing warnings and cease-and-desist declarations. If the infringer refuses to comply, the rights holder can apply to the court for an injunction, which may include not only cessation but also a contractual penalty for future infringements. In addition, claims for damages are possible, which are often calculated on the basis of the usual licence fees. The infringer is also obliged to provide information, but this is often difficult to enforce in practice.

In addition, copyright law protects technical measures (eg, encryption, DRM systems, geo-blocking) in accordance with Section 95a et seq. of the German Copyright Act. Circumventing such technical protection measures is prohibited.

The relevance of IP protection of data and databases is particularly evident in the context of artificial intelligence (AI). Training AI models requires large datasets that often contain copyrighted or sui generis protected database content. Using such data generally requires licenses or rights, as copying and analysing protected works during AI training may constitute infringement. However, German copyright law provides specific exceptions for text and data mining, especially for scientific research purposes (§§ 44a ff. and § 60d UrhG). Recent rulings by the Hamburg Regional and Higher Regional Court confirmed that AI training with protected data can be lawful if used for non-commercial research. These decisions – which are still subject to further legal and academic debate – suggest that certain research uses may be covered by the text and data mining exceptions.

However, commercial AI training and use without proper licences or rights remains legally problematic and may infringe copyright and/or database rights. Rights clearance and contractual arrangements with data and database owners are therefore a key element of legally compliant AI projects

Apart from copyright, individual data and/or data bases may also be protected by trade secret law. Data may be protected as trade secrets if it (1) has economic value, (2) is not generally known or readily accessible, and (3) the owner takes reasonable confidentiality measures (eg, restricting access rights, encryption, NDAs, etc.).

Therefore, it is essential to carefully consider the legal framework when using databases and data for AI training to respect copyright and minimise legal risks. For data owners and database producers, it is now all the more important to develop strategies to protect their datasets and databases under IP law.

Law stated - 1 January 2025

Third-party links and content

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

Under German and European law, linking to third-party websites or platforms generally does not require permission if the linked content is lawfully published and publicly accessible. Courts have ruled that providing a hyperlink alone usually does not amount to copyright infringement, as the content provider decides on making the content available to the public decides on public availability.

However, case law legal decisions also establishes that linking can lead to liability if the linked content infringes copyright or contains unlawful material —especially when the linking is done for commercial purposes and the operator either knew or should have known about the illegality. In such cases, website operators may be required have a duty to verify the legality of the linked content and remove links once if they become aware of infringements.

Thus, while linking without permission is mostly permitted, commercial operators must exercise due diligence to avoid liability. For non-commercial use, liability generally arises only if there is actual knowledge or suspicion of illegal content.

Law stated - 1 January 2025

27 | 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?

Generally, no – not without a legal basis or licence. A website, digital platform or other online content provider may not freely use third-party content merely because it is publicly accessible or has been obtained by automated scraping. The permissibility depends on

the type of content, the intended use, applicable licence terms, and whether the use falls within a statutory exception such as text and data mining under German copyright law.

Open content may be used without obtaining additional express permission from the third-party content provider where the content has been made available under a valid open licence, such as a Creative Commons licence, and the intended use complies with all applicable licence conditions. Depending on the licence, these conditions may include attribution, share-alike obligations, restrictions on commercial use, or prohibitions on derivative works.

Open content can be used on websites without express permission from the third-party content provider as long as the use complies with the terms of the licence in question (ie, Creative Commons). Where third-party (copyrighted) digital content is obtained or processed automatically, the relevant German copyright rule is section 44b of the German Copyright Act (UrhG). This provision permits certain reproductions of lawfully accessible works for the purpose of text and data mining. The statutory permission under section 44b UrhG applies only if the rights holder has not reserved the relevant use. For works made available online, such a reservation is effective only if it is made in machine-readable form.

That said, a website or online platform may use third-party content without separate permission only in limited circumstances, in particular where: the content is made available under an open licence and the use complies with the licence terms; the use is limited to text and data mining of lawfully accessible works under section 44b UrhG; the rights holder has not validly reserved the use in machine-readable form; and no other legal restrictions apply, such as database rights, contractual restrictions, data protection law or unfair competition rules. For uses going beyond analysis, especially publication, reproduction on a website, commercial exploitation, or substitution of the original content provider's offering, express permission or a suitable licence will usually be required. Furthermore, the automated use of digital content must not be expressly prohibited, as regulated by section 44b of the German Copyright Act (UrhG). However, such a prohibition must be stored in machine-readable form.

The unlawful use of content protected under IP rights without a licence may lead to legal action by the rights holder. In a first step, the rights holder will usually send a cease-and-desist letter. There is no immediate fine associated with receiving cease-and-desist letters. The only monies to be paid, initially, are legal and administrative fees by the rights holder prior to any court proceedings. The cease-and-desist letter usually requests the website owner to stop the infringement and sign an undertaking promising to pay a contractual penalty in case of culpable infringement with a penalty clause. If the website owner signs an undertaking and pays up the legal costs involved (usually between €300 and €2,000), the complaint will most likely not result in a court action as the claim will lose its substance. If the website owner signs a cease-and-desist declaration with a penalty clause and nevertheless continues its practice, then the contractual stipulated penalty or an amount established by the court of typically around €5,000 for the first infringement (also depending on scope, impact and gravity of the infringement) is due and payable to the contracting partner. If the website owner refuses to sign the cease-and-desist declaration, the rights holder may file for an interim injunction at a competent court. The court may grant the injunction with the cease-and-desist injunction combined with an obligation to pay a penalty for future infringements. The rights holder may also claim damages suffered by the infringement for the use of the content without a valid licence, which are calculated via

a licence fee analogy. In addition, the rights holder may assert claims for information, which are very burdensome in practice. If the infringement was intentional, the consequences can even be of a criminal nature, with an impending penalty of up to three years in prison.

Particularly in the case of automated scraping, also data protection issues can arise when personal data is reproduced or further processed. This is only permissible with explicit consent or a legitimate interest. The Cologne Higher Regional Court recently ruled that Meta may use publicly posted personal data of adult Facebook and Instagram users to train its AI model without consent, because this is justified by a legitimate interest. However, this decision provides only broad guidelines and cannot be applied to every context involving the web scraping and further use of personal data.

Law stated - 1 January 2025

Metaverse and online platforms

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

The metaverse presents new challenges for intellectual property (IP) protection under German law due to its immersive, decentralised, and cross-border nature. Although existing IP rules apply, their enforcement and practical application are complicated by the virtual context.

General Challenges:

- Determining applicable jurisdiction and law is complex due to cross-border operations of many metaverse platforms.
- The decentralised platforms and global accessibility often make traditional enforcement difficult.
- Terms of service often try to address IP, but their scope and enforceability vary.
- Blockchain technologies such as NFTs introduce new issues around proof of ownership and licensing, requiring adapted contractual agreements.

Regarding IP protection, German authorities, including the German Patent and Trademark Office (DPMA), affirm that IP laws apply equally in virtual spaces and emphasise the importance of developing strategies to protect IP rights in the metaverse. Businesses are advised to combine traditional IP protections with innovative licensing, monitoring, and enforcement schemes tailored for the metaverse context.

Law stated - 1 January 2025

Exhaustion of rights and first-sale doctrine

29 | 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?

Yes, all IP rights are subject to the concept of exhaustion or first-sale doctrine. It is a prerequisite that the product containing the IP rights has been placed on the market by the owner of the IP rights or with his or her consent in Germany, in one of the other member states of the European Union or in another state party to the Agreement on the European Economic Area. The concept of exhaustion or first-sale doctrine is explicitly also applicable to software. There is no similar provision for other digital products, therefore there is no concept of exhaustion or first-sale doctrine.

Whether the concept of exhaustion or first-sale doctrine applies to digital products placed on a metaverse therefore depends on whether the rights are embedded in software. Placing digital products on a platform in another territory does not affect the legal situation in Germany.

Law stated - 1 January 2025

Administrative enforcement

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

Criminal justice authorities can order freezing injunctions, as well as the search of premises and the confiscation of evidence in criminal investigation proceedings in connection with IP infringements.

Measures conducted by customs authorities, in particular border seizure procedures, are also of great practical importance.

Law stated - 1 January 2025

Civil remedies

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

Civil remedies include, in particular, claims for injunctive relief, removal and damages. Injunctive relief is often granted on an interim basis by preliminary injunction, which can be issued ex-parte within a few days after filing. German law also provides for a legal instrument comparable to freezing orders under British law if there is a real likelihood of assets leaving the country (arrest). However, this legal remedy is rarely applied in IP disputes.

In addition, legal remedies are available to the rights holder to counteract potential difficulties in gathering evidence: the information claim includes entitlement to demand information on the provenance and distribution channel of the infringing goods; the inspection claim includes entitlement to demand the submission of documents and the inspection of objects, provided there is a 'reasonable likelihood' of an infringement.

Law stated - 1 January 2025

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

- 32** | 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 term 'personal data' is defined in the General Data Protection Regulation (GDPR) as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Beyond that, the GDPR and German law refer to 'special categories of personal data' rather than 'sensitive data'. These comprise personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health as well as genetic or biometric data for the purpose of uniquely identifying a natural person. The processing of such special categories of personal data is, in principle, prohibited and only permitted under certain strict conditions (for example where an explicit legal basis applies or explicit consent has been obtained in accordance with article 9 GDPR).

Law stated - 1 January 2025

Registration and appointment of data protection officer

- 33** | 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?

Data controllers themselves do not have to register with any regulator; however, the controller shall designate a data protection officer if they constantly employ as a rule at least 20 persons who are permanently engaged in the the automated processing of personal data. The data protection officer must be named to the competent supervisory authority.

Law stated - 1 January 2025

Extraterritorial issues

- 34** | 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?

Yes, the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the

data subject is required, to such data subjects in the EU; or the monitoring of their behaviour as far as their behaviour takes place within the EU.

Where the above-mentioned applies, the controller or processor established outside the EU must, as a rule, designate in writing a representative in the EU. This representative must be established in one of the member states where the data subjects concerned are resident. Certain limited exceptions apply, for example where the processing is occasional, does not include special categories of data on a large scale and is unlikely to result in a risk to the rights and freedoms of natural persons.

Law stated - 1 January 2025

Bases for processing

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

There are no comprehensive statistics available on the most frequently used legal bases for processing.. From our experience, data processing is often based on the fulfilment of the contract, legal obligations or the legitimate interest of the controller. In addition, consent is obtained in many cases, unless another reason for processing is apparent.

With regard to transfers to third countries, the most commonly asserted bases include adequacy decisions of the European Commission and the use of Standard Data Protection Clauses (standard contractual clauses). In individual constellations, binding corporate rules or one of the derogations provided for in article 49 GDPR may be relied upon.

Law stated - 1 January 2025

Data export and data sovereignty

- 36** | 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?

When transferring data to another jurisdiction, a distinction must be made between EU member states and other jurisdictions. The transfer of data to other member states is based on the same rules as a data transfer within Germany, because the GDPR applies uniformly across the EU and transfers within the European Economic Area are not considered “transfers to third countries”. In the case of a transfer outside the EU, the corresponding provisions of the GDPR (article 44 et seq) must also be observed. In addition to ensuring that the underlying processing is lawful, the controller must verify that an appropriate transfer mechanism is in place for the specific destination country. Various options are available here. As a rule, the transfer to third countries is based on an adequacy decision of the European Commission or the Standard Data Protection Clauses. In addition, international corporations can introduce binding corporate rules. In individual cases, further legal processing options are available.

No general rules exist that require data, data servers or databases to remain in the German jurisdiction. Sector specific requirements may apply in isolated areas (for example in financial supervision or security related contexts), but there is no overarching data localisation regime in German data protection law.

Law stated - 1 January 2025

Sale of data to third parties

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

There is no specific German rule on selling personal data. The GDPR neither allows nor explicitly permits the selling of data to a third party. Licensing data requires a legal basis for the data processes. Consent might work. The debate is ongoing, if legitimate interest works regarding selling data, for example, as part of an M&A asset deal, if certain requirements are met. The party's liability is that they might violate the GDPR.

Law stated - 1 January 2025

Consumer redress

- 38** | 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?

Individuals have the right to transparent information, access, rectification, erasure, restriction of processing, data portability, to object to certain types of processing and not to be subject to a decision based solely on automated processing (articles 13 to 22, GDPR) in relation to the processing of their personal data. Damages resulting from an infringement of the GDPR have to be compensated (article 82, GDPR). These rights have to be complied with by all controllers or processors in the EU, regardless of the nationality of the individual or where the data is processed. The rights are not limited to EU citizens but apply to any individual whose personal data are processed under the GDPR, regardless of nationality. In practice, they apply to all individuals who are in the EU where goods or services are offered to them or whose behaviour within the EU is monitored.

Law stated - 1 January 2025

Non-personal data

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

Under German data protection law, section 25 of the German Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services (TDDDG)

applies to the access to and storage of information on end user terminal equipment, regardless of whether that information qualifies as personal data. This section is the German implementation of article 5 (3) of Directive 2002/58/EU (the Cookie Directive).

In accordance with section 25 (1) of the TDDDG, the storage of information in the end user's terminal equipment or access to information already stored in the terminal equipment shall only be permitted if the end user has consented on the basis of clear and comprehensive information. The information to the end user and the consent shall be provided in accordance with the GDPR (especially articles 7, 12, 13 and 14). 'Information' can be personal or non-personal data, so section 25 TDDDG effectively extends GDPR-style consent requirements to certain non personal data stored on or accessed from terminal equipment.

In accordance with section 25 (2) of the TDDDG, consent is not required if:

- the accessing or storing (or both) of information is solely necessary to carry out the transmission of a message over a public telecommunications network; or
- the accessing or storing (or both) of information is absolutely necessary for the provider of a telemedia service to be able to provide a telemedia service expressly requested by the user.

In addition, the EU Data Act establishes harmonised rules for fair data access and use across the Union. It regulates access to and use of data generated by connected products (such as IoT devices) and related services, covering manufacturers, service providers, users, and data holders, and applies when such products or services are offered in the EU. The Data Act covers both personal and non personal data; where personal data are concerned, its provisions apply in addition to, and without prejudice to, the GDPR.

Law stated - 1 January 2025

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

In general, documents can be archived digitally. The most common laws and regulatory guidelines with regard to archiving of documents do not explicitly require documents to be archived in paper form. However, there are laws that require documents to be archived in their original form, which therefore may require the documents to be archived in paper form. This is most prominently the case for annual financial statements, opening balance sheets and certain documents in customs procedures (information to the customs authorities and supporting documents required for the application of the provisions governing the customs procedure), according to section 147(2) of the German Fiscal Code. Other documents, such as commercial mail or receipts must be stored in such a way that their reproduction corresponds visually to the original.

In explicitly listed cases, the law requires documents to be notarised in order to become valid, in particular regarding the acquisition of real estate, the founding of particular legal

corporations (GmbH) or the transfer of shares in such a legal corporation. The German legislator has provided new regulations that all notarised deeds have to be archived additionally in an electronic vault of deeds. Still, this will not remove the obligation to archive the original deed as well.

Original digital documents such as electronic invoices must be kept in the digital original; they may not be changed or deleted within the retention period, and a tax auditor must be able to evaluate them mechanically.

The question of the obligation to retain certain documents as original documents must be distinguished from the probative value of documents. Under German procedural law, the probative value of original documents is often considered higher than that of electronic copies (presentation of the original or certification of a copy may be required). For this reason, it might be advisable to (additionally) retain the original documents even if there is no obligation to retain them.

The probative value should especially be considered with regard to contracts, which are subject to the written form requirement according to section 126 of the German Civil Code. While the written form ('wet ink on paper') as required by respective laws and contracts can basically be replaced by a qualified electronic signature according to section 126a of the German Civil Code, there are [technical aspects regarding the archiving of such documents](#) that need to be considered. As of 2025, German law has simplified the requirements for written form in particular in the prominent areas of labour and rental law: Employment contracts, job references and certificates, job conditions and employee leasing agreements as well as commercial lease agreements and rental agreements regarding property not used for living do not require written form on a physical piece of paper any more but may be agreed in electronic form (text form).

Any archiving of documents should always be in line with the [banking authorities' principles of proper accounting](#).

Law stated - 1 January 2025

Retention

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

The most important laws regarding the archiving of documents are section 147(3) of the German Fiscal Code and section 257(4) of the German Commercial Code. They require archiving of documents for six, eight or 10 years. However, data privacy laws may require you to block access to these documents during the retention periods, in case they contain personal data which are not eligible to be accessed by everyone after a certain period of time.

According to German tax law, all business documents that are of importance for understanding and verifying the records required by law must be kept for either six, eight or 10 years. Section 147(1) of the German Fiscal Code lists the individual documents that must be kept, namely:

- accounts and records, inventories, annual financial statements, situation reports, the opening balance sheet and the operating instructions and other organisational documents needed for their comprehension;
- trade or business letters received;
- reproductions of trade or business letters sent;
- accounting records;
- information to the customs authorities and supporting documents required for the application of the provisions governing the customs procedure; and
- other documents to the extent that these are of relevance for taxation.

According to section 257 of the German Commercial Code, the retention period for books and records, annual accounts, inventories, management reports, opening balance sheets, accounting vouchers, documents required to be attached to a customs declaration made by means of a data processing technique where the customs authorities have waived their presentation or returned them after presentation shall be 10 years. As of 2025, invoices and cost vouchers only need to be retained for eight years. All other business documents subject to retention shall be retained for six years. The period always begins with the expiry of the calendar year in which the last entries, changes or actions were made in the respective documents, or commercial letters were received or dispatched. In the case of contractual documents, the period begins after the expiry of the contract.

In addition to the central tax law provision of section 147(1) of the German Fiscal Code, German law contains further retention obligations in special laws (ie, banking laws) that apply to specific documents and specific industries. Anti-money laundering laws for example require the retention of relevant documentation (can be stored digitally) regarding contracting parties, transactions and risk assessments for at least five years (section 8(4) Money Laundering Act). In this respect, an examination of the individual case is always necessary.

Further documents that are required for the assertion of legal claims can and should be archived for at least three years (regular statute of limitations).

Law stated - 1 January 2025

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

All companies must protect personal data according to the General Data Protection Regulation (GDPR), and in accordance with the German Act on Data Protection and Protection of Privacy in Telecommunications and Digital Services (TDDDG).

This also applies to internet transactions. Encryption is not mandatory, but it is regularly a suitable measure according to article 32 of the GDPR. In addition, providers of internet or telecommunications services (for example, internet service providers) must take appropriate technical measures to protect against disruptions (section 19(4), TDDG; section 165, German Telecommunications Act).

With regard to the implementation and maintenance of appropriate measures, the state of the art must always be taken into account; in other words, the requirements automatically increase with technical progress. However, German law does not specify details, such as encryption algorithms or key lengths.

Law stated - 1 January 2025

Data breach notification

- 43** | 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?

The general rules of the GDPR regarding data breach notification apply for e-commerce as well. In particular, article 4 (1) and (12) GDPR (defining personal data and what a breach of personal data is), article 32 GDPR (technical and/or organisational measures to protect personal data), articles 33 and 34 (setting the rules for notifications and communication about personal data breaches). Furthermore, articles 82 (implementing a damage claim for affected data subjects) and 83 (imposing severe fines for infringing the applicable rules) GDPR are applicable.

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (article 4 (12) GDPR). Data breaches have to be reported in general, if there is a risk that somebody from outside or inside an organisation has gained unauthorised access to the personal data of an EU citizen. The controller or processor has to scrutinise the incident as well as the potential consequences.

Any such violations of the privacy of personal data have to be notified to the supervisory authorities unless the risks for affected persons are excluded (eg, due to encryption). The reporting has to take place within 72 hours with concrete information as well as additional documentation of the incident and the countermeasures taken (there might be a change regarding the relevant time period in the future).

If there are in addition high risks to the rights and freedoms of natural persons (eg, financial and social harm, identity theft or professional secrecy), the controller has to inform the person concerned immediately, unless technical protection against the risks (eg, encryption) is provided. The supervisory authority may order the publication of a public notice of the incident.

A breach of reporting obligations in the event of data breaches can be sanctioned with a fine of up to €10 million or 2 per cent of the annual turnover achieved worldwide, whatever is higher. Moreover, data subjects affected by the data breach are entitled to claim material

and even immaterial damages caused by the controller's failure to report to the regulators and inform the data subjects in a timely manner.

Law stated - 1 January 2025

Government interception

- 44** | 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?

Authorities cannot require users to reveal their private keys used for encrypted communications. Certification authorities are permitted. Their operation is regulated by the Regulation (EU) 910/2014 of 23 July 2014 (the eIDAS Regulation) and supplementary national law, in Germany the Trust Services Act. Liability is regulated in articles 11 and 13 of the eIDAS Regulation. If the trust service provider contracts with third parties, liability is increased according to section 6 of the German Trust Services Act.

Law stated - 1 January 2025

GAMING

Legality and regulation

- 45** | 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?

In Germany, any kind of gambling, including online betting and fortune-based gaming business, is generally forbidden, with only specific exceptions that are heavily regulated under the State Treaty on Gambling and require a state licence to operate in the German market. By definition under the State Treaty, gambling requires a kind of consideration for participation (betting or gambling for free or without wager therefore does not fall under the regulatory scheme). It is currently subject to court cases if the consideration needs to reach a certain amount or level for the definition to apply. After a long period of legal uncertainty due to European jurisdiction regarding the old State Treaty, Germany finalised its new State Treaty on Gambling, which entered into force in July 2021. Under the new State Treaty, it is now generally possible to also acquire licences for online casinos, online poker and virtual slot machine games (besides lotteries, sports betting and horse betting). The State Treaty on Gambling stipulates a multitude of prohibitions and requirements for the acquisition of an official licence. Requirements of any such licence under the State Treaty include participation in a digital prevention system, extensive monetary securities and background checks. Any advertisement for unlicensed gambling is strictly forbidden and may also constitute a criminal offence (as can the operation of any unlicensed gambling activity). The same may apply to payment service providers in regards to unlicensed gambling of any kind. The competent authority in Germany is the Joint Gambling Authority (*Gemeinsame Glücksspielbehörde der Länder*) in Halle (Saale), Saxony-Anhalt.

Law stated - 1 January 2025

Cross-border gaming

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

It is only permissible to advertise, or provide access to, an online betting or gaming business in the German market that is licensed in Germany. Licences of other jurisdictions do not hold any validity in Germany in this regard, since the new State Treaty on Gambling came into force in July 2021. If the respective metaverse is considered to address the German market, the same applies. However, if online betting or gambling businesses in other jurisdictions are accessible from Germany but do not address the German market (eg, you cannot participate from Germany or register to the service with a German address), German regulation might not apply.

Law stated - 1 January 2025

OUTSOURCING

Key legal issues

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

It is highly important to define the exact scope of the services and the quality. The quality is normally provided in service level agreements. The agreement has to contain specific provisions as to the cooperation obligations of the customer. Other key issues are provisions regarding the migration of data and the cooperation of the service provider after termination of the contract to switch to a new service provider.

Law stated - 1 January 2025

Sector-specific issues

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

As far as data is concerned, where there is a professional secrecy obligation or where sensitive data according to the General Data Protection Regulation is concerned, additional rules have to be complied with. Banking is the other area in which additional requirements have to be complied with (eg, MaRisk).

Law stated - 1 January 2025

Contractual terms

- 49** | Does the law require any particular terms to be included in outsourcing contracts?

As there is no general outsourcing law, there is no such requirement. However, there are sector-specific regulations – for example, in banking there are requirements as to the minimum regulations an outsourcing agreement has to contain (eg, European Banking Authority Guidelines, MaRisk) or in the financial sector the Digital Operational Resilience Act (DORA).

Law stated - 1 January 2025

Employee rights

- 50** | 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?

If an operation or part of an operation is moved to the service provider, the employment contracts of the relevant employees are moved to the service provider by power of law. The employees have to be informed in advance. The employees have the right to object to the transfer of their employment.

Law stated - 1 January 2025

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

At the EU level, the Artificial Intelligence Act (Regulation (EU) 2024/1689) entered into force on 1 August 2024, introducing a harmonised framework for the placing on the market, putting into service and use of AI systems in the EU. The regulation adopts a risk-based approach, classifying AI systems as prohibited, high-risk, limited-risk, or minimal-risk.

Prohibited AI practices, such as social scoring or manipulative subliminal techniques, are banned since 2 February 2025. High-risk AI systems remain permissible but are subject to strict requirements, including risk management, high-quality training data, technical documentation, human oversight, conformity assessment and registration in an EU-wide database. Providers must ensure lifecycle traceability and compliance with extensive governance standards. At the time of writing, the application dates for certain obligations relating to high-risk AI systems are subject to ongoing legislative amendments under the EU's proposed AI Omnibus initiative. If adopted, these amendments are expected to postpone the application of certain obligations for high-risk AI systems.

The AI Act also regulates general-purpose AI models (GPAI), including large language models. As of 2 August 2025, GPAI providers must comply with transparency, documentation, copyright and risk mitigation obligations. Additional obligations apply to

GPAI models that pose systemic risks. A transitional period until 2 August 2027 applies for GPAI models already placed on the market.

The AI Act operates in parallel with the GDPR, which remains fully applicable wherever personal data are processed. This includes compliance with the principles of lawfulness, purpose limitation, data minimisation, and transparency. One particular challenge is the difficulty of relying on consent under article 6(1)(a) or article 9(2)(a) GDPR, since such consent can be withdrawn at any time, and training data typically cannot be extracted from a model once incorporated.

Furthermore, article 22 GDPR restricts decisions based solely on automated processing, including profiling, that produce legal effects or similarly significant consequences for the individual. Although limited exceptions exist, their applicability in practice is often uncertain.

Under article 35 GDPR, a data protection impact assessment (DPIA) is required where the use of new technologies is likely to result in a high risk to the rights and freedoms of natural persons. This includes systematic and extensive profiling or automated decision-making with significant legal or practical impact on individuals.

On a national level, there is no legislation in place specifically addressing training using AI systems. However, the development, training, deployment and use of AI systems must comply with the general legal framework in Germany, including copyright law. In particular, training data may be protected by copyright under the German Copyright Act (UrhG), requiring appropriate licensing from the rights holder. In addition, training data may be subject to statutory or contractual confidentiality obligations, rendering them unsuitable for use in AI training.

Where personal data are involved in the training of AI models, the requirements of the General Data Protection Regulation (GDPR) apply.

Law stated - 1 January 2025

IP rights

- 52** | 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 can be protected by the UrhG as a representation of a scientific or technical nature according to section 2, paragraph 1, No. 7 of the UrhG, as a database according to section 4, paragraph 2 of the UrhG, section 87a et seq of the UrhG, and the German Trade Secrets Act.

However, the protection of products created by AI is problematic under the current legal framework. This is best illustrated using the example of German Copyright Law: according to section 2, paragraph 2 of the UrhG, copyright exists only for personal intellectual creations. For the copyrightability of a product, it is therefore decisive whether and to what extent it can be traced back to the creative activity of a natural person. Thus, pure AI works are not works within the meaning of section 2, paragraph 2 of the UrhG. However, if the AI

work is edited by a natural person and thus achieves a corresponding level of design, it can enjoy copyright protection. Consequently, the more autonomously the AI works on such a creation, the less likely it is that it will be protected by copyright. While there is a discussion in German legal literature, whether prompts (eg, prompts entered in AI-powered chatbots or large language models) may lead to some kind of copyright in the results returned by the AI, the prevailing view is that this is not the case.

Law stated - 1 January 2025

Ethics

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

The EU AI Act is based on a risk-based approach that categorises AI systems into four categories, each of which is subject to a different level of regulation: minimal risk, limited risk, high-risk and prohibited (unacceptable risk) AI practices. Examples include certain real-time remote biometric identification AI systems in publicly accessible spaces (subject to limited exceptions) and AI systems used for prohibited social scoring.

For the remaining three risk categories, the higher the risk, the more extensive the legal requirements. For example, AI systems that are considered high-risk are not prohibited but are subject to stringent requirements with respect to their development, distribution and deployment. The AI Act imposes various obligations on developers and distributors, including with respect to quality and risk management, technical documentation, and oversight, robustness, safety, and accuracy of the AI system. Such AI systems must also be registered in an EU-wide database.

For AI systems with limited or minimal risk, the AI Act primarily provides for certain transparency requirements and notification obligations.

Law stated - 1 January 2025

TAXATION

Online sales

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

There are no special rules for German income and corporation tax in relation to digital products and online services; the so-called *Betriebsstättenansatz* (permanent establishment approach) applies. The ordinary income or corporation tax rate applies to all profits from these transactions made from a German permanent establishment. This principle remains unchanged as of July 2025.

However, a distinction has been made for value added tax (VAT): In case of online sales (e-commerce), the decisive factor is whether the entire transaction is carried out via internet (ie, ordering and delivery of the item) or whether only the order is placed via internet and

delivery is carried out in the conventional manner (ie, by mail). Only the first case is an "online turnover" according to sec. 3 a (4) No. 14 UStG (Value Added Tax Act), the second case is a normal mail order business in the form of a movement of goods ("offline turnover").

Both transactions are taxable. The download of software is an electronic service that is generally provided at the place of residence of a private individual in an EU country and is subject to VAT in accordance with local VAT law (sec. 3 a (5) UStG). Therefore, a download by a German citizen from a server in another EU country is (also) subject to German VAT. Nonetheless, for companies VAT has to be paid in the country in which the company is based, ie, VAT only has to be paid in Germany for companies based in Germany, regardless of where a server is located. As of July 2025, no significant changes have occurred in this area since the implementation of the VAT Digital Package in 2019 and 2021.

Law stated - 1 January 2025

Server placement

- 55** | 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?

Under German law, a server constitutes a permanent establishment that is taxable in Germany if the functions performed on the server or at the location are "significant and essential" or are attributable to the core part of the entity's operations. However, an additional crucial criterion applies: the company must have discretionary power (-*Verfügungsmacht*) over the server. This discretionary power exists if the server is owned by the company or if the company is assigned a specific server for its exclusive use.

German tax authorities regularly assume a significant and essential function if it is not merely an ancillary or auxiliary activity.

A foreign company with a dedicated server that is (still) located on German soil therefore establishes a permanent establishment in Germany provided the company has discretionary power over the server. If the company merely has a claim to the provision of computing capacity (eg, through cloud hosting services), discretionary power is typically lacking, and no permanent establishment is established. Conversely, however, operating a platform for the German market or a virtual market is not sufficient to establish a permanent establishment in Germany if there is no physical connection to German soil. This assessment remains valid as of July 2025.

Nevertheless, with regard to VAT, serving the German market may be sufficient to trigger German VAT (see above).

Law stated - 1 January 2025

Electronic invoicing

- 56** | 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?

The German tax law contains detailed regulations on the requirements on invoices. Sec. 14 (1) UStG stipulates expressly which information must be included in a so-called *elektronische Rechnung* (e-invoice) or *sonstige Rechnung* (other invoice).

The *Wachstumschancengesetz* (Growth Opportunities Act) has revised the regulations governing the issuance of invoices in accordance with sec. 14 UStG for transactions carried out after 31 December 2024. Since 1 January 2025, so-called *verpflichtende elektronische Rechnung* (mandatory e-invoices) must be used for transactions between domestic entrepreneurs or companies. An entrepreneur in this sense is anyone who independently carries out a commercial or professional activity (sec. 2 UStG). This also includes, for example, freelancers or persons who exclusively provide tax-exempt transactions, such as landlords, small business owners or doctors. A domestic company is defined as a company that has its registered office, management or a permanent establishment involved in sales within the territory of the Federal Republic of Germany. If there is no registered office, the entrepreneur's place of residence or habitual abode applies.

However, since 1 January 2025, an *E-Rechnung* is only considered to be an e-invoice if it is issued, transmitted and received in a structured electronic format, that comply with the EU standard for electronic invoicing and the list of corresponding syntaxes (CEN standard EN 16931), and can be processed electronically. This means invoices that are sent in a different digital format (PDF, JPG, etc.) are not considered to be an e-invoice because it does not have a structured format. Invoices that do not meet the requirements for an e-invoice have been referred to as 'other invoices' since 1 January 2025. In particular, invoices on paper or in an unstructured electronic format (eg, simple PDF document) constitute such other invoices.

Still, an e-invoice only needs to be issued if the transaction was carried out on or after 1 January 2025. E-invoicing is not mandatory for transactions carried out before this date. However, the e-invoicing requirement only applies if there is a VAT obligation to issue an invoice in the first place. Therefore, the regulations do not apply. In these cases, issuing an invoice is generally voluntary from a VAT perspective. However, even if there is a VAT obligation to issue an invoice, it does not necessarily have to be issued as an e-invoice in the following cases:

- Small amounts (up to EUR 250 (before tax), sec. 33 VAT Implementation Regulation *UStDV*),
- Travel tickets that are considered invoices (sec. 34 UStDV),
- Services provided by small businesses (sec. 34a UStDV),
- Services to legal entities that are not entrepreneurs (eg, many associations or state institutions), and
- Certain services to end consumers in connection with a property.

In these cases, other types of invoices may continue to be issued.

Nevertheless, transitional provisions will apply until 31 December 2026. During the period from 1 January 2025 to 31 December 2026, all invoice issuers may choose to issue a non-electronic invoice instead of an e-invoice. However, as before, a non-e-invoice in a different electronic format than an e-invoice (eg, email with a PDF file) can only be used

if the recipient agrees to this format. The reason for this is that the recipient cannot be expected to accept an electronic format that is completely unfamiliar to them. Moreover, if the invoice issuer's turnover in the previous year was less than €800,000, this period is extended until the end of 2027.

In any case, paper, digital and e-invoices in Germany have each to be stored. According to sec. 14b (1) UStG, entrepreneurs are required to retain a copy of every incoming and outgoing invoice for eight years. In the case of e-invoices, at least the structured part must be retained in such a way that it remains intact in its original form.

No taxpayer in Germany is obliged to submit copies of invoices to the tax office or any other authority without being asked to do so. Nevertheless, taxpayers are obliged to keep copies of invoices and to present them on request, particularly in the context of a tax audit. As of July 2025, the planned electronic reporting system (*Meldesystem*) for transmitting invoice data to tax authorities has not yet been implemented.

Companies can submit e-invoices to the tax authorities via the so-called *ELektronische STeuer ERklärung (ELSTER)* system. To do so, they can use the “-*Belegnachreichung zur Steuererklärung*” (submit documents for tax return) function (-www.elster.de/eportal/formulare-leistungen/alleformulare/belegnachreichung) and upload the e-invoice there under “5-Anhänge” (five attachments). Furthermore, invoices to public authorities (so-called B2G transactions) are not subject to the VAT regulations for mandatory e-invoicing if the authority is not acting as a company. However, since 27 November 2020, suppliers and service providers have already been obliged to issue electronic invoices to public contracting authorities on the basis of the e-invoicing regulations.

Law stated - 1 January 2025

DISPUTE RESOLUTION

Venues

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

There are no dedicated specialist courts in Germany that deal exclusively with online or digital law issues. Digital and online related disputes are heard by the ordinary civil courts (and, where relevant, administrative or criminal courts), applying the general rules of civil procedure and substantive law. While some courts have chambers or panels that focus on particular subject matters (for example commercial or IP law), there are currently no permanent specialist chambers devoted solely to online or digital disputes.

Law stated - 1 January 2025

ADR

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

The European Online Dispute Resolution platform was discontinued with effect from 20 July 2025. Its closure, following relatively low case numbers across the EU, underlines that EU level online ADR mechanisms have not played a major practical role for consumer disputes in Germany. However, ADR more broadly is available for online/digital disputes through the existing network of recognised consumer dispute resolution bodies and other sector specific schemes.

Nevertheless, online retailers are still required (§ 36 VSBG) to state on their website and in their terms and conditions whether they are willing or obligated to participate in alternative dispute resolution. If applicable, they must also provide information about the relevant consumer arbitration body. Participation in ADR remains generally voluntary for businesses, unless specific legislation or contractual arrangements provide otherwise, and ADR is therefore not yet a predominant method of resolving online/digital disputes in Germany, although its use is gradually increasing in certain sectors (for example platform and copyright related disputes where specialised ADR schemes exist).

Law stated - 1 January 2025

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

The EU's digital regulatory framework has undergone significant transformation in recent years. The focus has now shifted from the adoption of new legislation to the implementation, enforcement and practical application of an increasingly comprehensive body of EU digital regulation. Businesses operating in Germany are required to comply with a growing number of directly applicable EU legal instruments, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Data Governance Act (DGA) and the Data Act.

Artificial intelligence remains one of the most important regulatory topics. The AI Act entered into force on 1 August 2024 and is being implemented in phases. The rules on prohibited AI practices and AI literacy obligations have applied since February 2025, while the provisions governing general-purpose AI models have applied since August 2025. Following the adoption of the EU's Digital Omnibus on AI, the application of the rules for stand-alone high-risk AI systems has been postponed until 2 December 2027 and, for AI systems embedded in regulated products, until 2 August 2028. Despite these revised timelines, the AI Act already has a significant impact on the development, procurement and deployment of AI systems and has become a key compliance priority for businesses.

Another major regulatory development is the Data Act, which has applied since 12 September 2025. The Data Act fundamentally reshapes the legal framework for connected products and related services by introducing extensive rights and obligations concerning access to and use of data. It has significant implications for contractual arrangements relating to data access, data sharing, cloud switching, interoperability and

business-to-business data transactions. Together with the Data Governance Act, it forms a central pillar of the EU's emerging data economy framework.

Cybersecurity has become another major focus of digital regulation. In particular, the Cyber Resilience Act (CRA) fundamentally changes the regulatory framework for manufacturers of products with digital elements, including software, SaaS components and connected devices. The CRA introduces mandatory cybersecurity requirements throughout a product's lifecycle, including secure-by-design principles, vulnerability handling, coordinated vulnerability disclosure, security updates, technical documentation and conformity assessment. As businesses prepare for the application of the CRA, cybersecurity considerations are increasingly influencing product development, software engineering, procurement and contractual risk allocation.

In parallel, Germany has implemented the NIS2 Directive, significantly expanding cybersecurity, governance and incident management obligations for essential and important entities. Together, the CRA and NIS2 are driving a substantial increase in cybersecurity compliance requirements across both the public and private sectors.

Overall, the key challenge for businesses is no longer monitoring new legislative proposals but implementing effective compliance programmes across an increasingly interconnected regulatory landscape. Artificial intelligence, data regulation and cybersecurity have become the defining pillars of digital regulation in Germany, requiring organisations to adopt integrated legal, technical and organisational compliance strategies rather than addressing each regulatory regime in isolation.

**The authors wish to thank Fabian Bauer, Corinna Schneiderbauer, Veronika Gelser, Moritz Mehner, Thomas Hausbeck, Maximilian König and Oliver M. Bühr for their assistance in the preparation of this chapter.*

Law stated - 1 January 2025



Franziska Ladiges
Matthias Orthwein
Stefan Peintinger
Johannes Schäufele
Daniel Meßmer

f.ladiges@skwschwarz.de
M.Orthwein@skwschwarz.de
s.peintinger@skwschwarz.de
j.schaeufele@skwschwarz.de
D.Messmer@skwschwarz.de

SKW Schwarz

[Read more from this firm on Lexology](#)

Hungary

[Endre Várady, János Tamás Varga](#)

[VJT & Partners](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The Hungarian government remains proactive in promoting digital transformation. It has adopted a number of strategic policy documents, including the National Digitalisation Strategy (2022–2030), the renewed National Artificial Intelligence Strategy (2025–2030), which is subject to annual review and updating, and the National Cybersecurity Strategy (2025–2030). Together, these strategies aim to strengthen Hungary's digital economy, AI adoption, cybersecurity resilience and digital public services. The government has also announced a broader review of Hungary's digital regulatory framework, with planned initiatives covering, among others, the governance of national data assets, AI-generated disinformation, the protection of children in the digital environment, and the establishment of new institutional structures supporting digital innovation and cybersecurity

Law stated - 4 August 2026

Legislation

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

The Hungarian [E-Commerce Act](#) and the Hungarian [Civil Code](#) set the main legal framework for the Hungarian digital business. In business-to-consumer (B2C) relations, special consumer protection regulation applies, including the regulation of unfair consumer practices and B2C contracts. In relation to platforms, special additional rules apply, including the implementation of the Copyright Directive and Audiovisual Media Services Directive. A wide variety of sector-specific regulations also apply depending on the nature of the digital product (eg, fintech regulation or the on-demand media regulation). The regulatory landscape is also increasingly shaped by new horizontal EU digital legislation, including cybersecurity and artificial intelligence rules, which complement the traditional legal framework depending on the nature of the digital service.

Law stated - 4 August 2026

Regulatory bodies

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

The supervision of the digital business area is allocated among different regulatory bodies depending on the type of legal field. The main regulatory bodies include the following:

- the [Data Protection Authority](#) (data protection);
- the [Consumer Protection Authority](#) (digital consumer protection);
- the [Hungarian Competition Authority](#) (digital consumer protection/digital competition);
- the [Media and Infocommunications Authority](#) (internet access tariffs /anti-spam, digital content, and telecoms); and
- the AI market surveillance authority and AI notifying authority (AI Act compliance and conformity assessment).

Law stated - 4 August 2026

Jurisdiction

- 4 | 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?

It depends on the nature of the relationship:

- In business-to-business relations, parties have the freedom to agree on the jurisdiction.
- In business-to-consumer relations, in principle, the jurisdictional clause of the general terms will be invalid.

In the latter case, the default rules of private international law apply:

- In EU cross-border selling, while businesses may file a proceeding against a Hungarian consumer only in a Hungarian court, the consumer may bring the proceeding against the business in a Hungarian court or the court of the EU member state where the business is domiciled.
- In non-EU cross-border selling (when the business is domiciled outside of Hungary), the jurisdiction is determined based on Hungarian national private international law.

Law stated - 4 August 2026

Establishing a business

- 5 | 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?

There is no substantial difference between the establishment of online businesses and brick-and-mortar businesses.

In general, there is no general permit requirement for pursuing online business, but like any other commercial activity it must be reported to the notary based on the business' registered office. In addition, for certain online businesses (eg, fintech companies, video-sharing content providers) additional sector-specific notifications and licences may apply.

It is important to highlight that some products (such as tobacco, veterinary medicine and dangerous products) may not be sold online.

Law stated - 4 August 2026

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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, it is possible. In the case of exchange of email or other equivalent individual communications, the contract is formed when one party clearly declares its offer (indicating the key terms) and the other party approves the offer. In the case of other forms of distance contract, the business must acknowledge the user's order within 48 hours by electronic means (otherwise the user is relieved from any contractual commitment).

'Click-wrap' contracts are generally enforceable if the user can review the terms and give their affirmative acceptance (eg, by ticking the checkbox).

Law stated - 4 August 2026

Applicable laws

- 7 | 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?

Choice of law

In general, based on the Rome I Regulation, digital contracts may not derogate from the Hungarian mandatory provisions with regard to choice of law where business-to-consumer (B2C) contracts apply, and the overriding Hungarian mandatory provisions where business-to-business (B2B) contracts apply.

Language

With regard to B2C contracts, the Hungarian consumer protection authority requires the Hungarian language based on the general fairness principle. With regard to B2B contracts, the Hungarian language is not a requirement, but in the case of platform-to-business

contracts, it is possible that the competent Hungarian authority will require the Hungarian language based on the fairness and transparency principle.

Forum

It depends on the nature of the relationship:

- in business-to-business relations, parties have the freedom to agree on the jurisdiction; and
- in business-to-consumer relations, in principle, the jurisdictional clause of the general terms will be invalid.

In the latter case, the default rules of private international law apply:

- in EU cross-border selling, while businesses may file a proceeding against a Hungarian consumer only in Hungarian court, the consumer may bring the proceeding against the business in Hungarian court or the court of EU member state where the business is domiciled; and
- In non-EU cross-border selling (when the business is domiciled outside of Hungary), the jurisdiction is determined based on Hungarian national private international law.

Law stated - 4 August 2026

Electronic signatures

- 8 | 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?

A legal document will be qualified as written if (1) it can be proved that the content of the document is unchanged, (2) the signatory is identifiable, and (3) the time of signature is identifiable. Where a written form is required (such as sale agreements or copyright agreements), parties shall primarily use a qualified electronic signature and time stamp or advanced electronic signature and time stamp. As a general rule, other forms of agreement such as agreements made via DocuSign or AdobeSign, exchange of emails or clicking an acceptance button, shall not be qualified as "written" agreements.

E-signature services must be provided by a [trusted service provider](#) registered in Hungary or another EU country.

Law stated - 4 August 2026

Breach

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

In the context of business-to-consumer online sales, consumers may withdraw from an electronic contract within 14 days. Businesses must adequately inform consumers about this right, otherwise the withdrawal deadline will be extended up to 12 months.

Based on the Hungarian implementation of EU Directive 2019/770 and 771, effective from 1 January 2022, consumers have new special remedies in the context of non-conformity of goods with digital elements, digital content and digital services (hereinafter: digital products). The consumer may ask to bring the digital products to conformity (unless it is impossible or would impose disproportionate costs). If the business fails to do so, the consumer may request a proportionate reduction in price or terminate the contract. The rule of reversal of burden of proof (ie, the consumer does not have to prove that the item was defective at the time of supply, as it is assumed by law) is extended from six months to one year in the case of digital products.

There is no special forum for dispute resolution available for the breach of digital contracts. General dispute resolution mechanisms, including the consumer conciliation boards and the competent courts, remain available.

Law stated - 4 August 2026

FINANCIAL SERVICES

Regulation

- 10** | 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?

The Central Bank of Hungary supervises this area. Apart from the general Hungarian advertising law, additional sector-specific rules apply to some bank products such as credit or advisory services (eg, in commercial communication any wording should be avoided that could create false expectations for the consumer about the availability or cost of credit, and bank-tied agents may not use the term 'adviser' in the commercial communication). The Central Bank of Hungary has the power to ask electronic communication service providers to block websites on which unauthorised financial services are advertised. In addition, the Central Bank of Hungary's Recommendation 13/2025 sets out supervisory expectations regarding the digital transformation and digital availability of financial products and services.

Law stated - 4 August 2026

Electronic money and digital assets

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

Hungary has implemented the E-Money Directive (EMD2) (2009/110) and Payment Services Directive (PSD2) (2015/2366), based on which customers may initiate transactions via their fintech providers instead of traditional banking industry players.

Fintech providers' services are subject to heavy Hungarian financial regulation (such as compulsory authorisation by the financial regulator and rules on strong customer authentication). As it is challenging for fintech providers to fully adjust to Hungarian legal requirements, the Hungarian financial regulator, the Central Bank of Hungary created a regulatory sandbox in which fintech providers can test their services in a controlled environment under the regulator's supervision.

Hungary has also implemented the EU's Markets in Crypto-Assets Regulation (MiCA), laying down rules for crypto-asset services.

Law stated - 4 August 2026

Digital and crypto wallets

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

There are currently no Hungary-specific restrictions on the ownership or use of crypto wallets or other methods of digitally storing crypto-assets. The previous national validation regime for crypto-asset conversion transactions has been repealed. Crypto-asset service providers remain subject to the EU's Markets in Crypto-Assets Regulation (MiCA).

Law stated - 4 August 2026

Electronic payment systems

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

There is no unified law on electronic payment transactions – the rules are scattered in various sector-specific financial regulations, as there are separate rules for various e-payment solutions such as instant payment, point-of-sale terminal payment and contactless payment. The implementation of the Payment Services Directive ((EU) 2015/2366) (PSD2) in Hungary and the introduction of multi-factor authentication significantly enhanced the security of electronic payment.

As of January 2021, merchants operating online cash registers are obliged to provide consumers with the possibility of electronic payment.

The volume of electronic payment transactions in Hungary is constantly growing. Hungary's instant payment system (AFR), has significantly supported real-time domestic electronic payments. The Central Bank of Hungary aims to stimulate electronic transactions by bringing continuously new packages of legislation. Under its Payments 2030 Strategy, it aims to increase the share of electronic transactions to 60 per cent, or to two-thirds with additional policy measures, by 2030.

Regarding third-party access to digital information in bank accounts, the rules on bank secrecy must be observed. PSD2 also introduced regulated third-party access (with

customer consent) to bank accounts for account information and payment initiation services, which are subject to licensing and oversight by the Central Bank of Hungary.

Law stated - 4 August 2026

Online identity

- 14** | 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 client's identity may be checked online by the third party if the customer due diligence requirements set out in the AML Act are observed.

If the third party is established outside the EU, the third-party customer due diligence report may be accepted only under specific conditions (eg, the third-party service provider applies the customer due diligence requirements set out in the AML Act and is supervised in accordance with the requirements).

The service provider may not accept the customer due diligence report of the third party if that party is established in a non-EU country with high risk.

The Central Bank of Hungary acts as the AML supervisory authority for financial institutions, fintech firms and crypto-asset service providers, overseeing compliance, licensing and enforcement. AML arrangements are assessed as part of the authorisation process and remain subject to ongoing supervisory review.

Law stated - 4 August 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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?

In a nutshell, the process is the following (in the below chronological order):

- check the availability of the domain name;
- choose the registrar who will be the service provider for the applicant;
- conclude the contract with the registrar;
- pay;
- accept the domain registration policy;
- check the technical requirements;
- check the fulfilment of the domain registration policy;

- grant the right conditionally (within one business day); and
- grant the final right of domain (if no complaint has arrived within eight days of granting the right conditionally).

Citizens of any country can apply for a second-level public domain name. For a first-level domain name, only citizens and legal entities from certain countries can apply. There is an [official .hu domain name registry](#) with information on the domain registration process and the list of countries from which a domain can be registered directly under .hu.

Law stated - 4 August 2026

IP ownership

- 16** | 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?

Domain names do not automatically confer any additional IP rights.

There is no obstacle to the registration of a domain name as a trademark, but the registered domain name does not itself constitute a legal basis for obtaining trademark protection without any further conditions. For the registration of the domain name as a trademark, a separate proceeding must be completed in line with the Trademark Act.

Further, domain names are rarely copyrightable as they are usually too short to qualify as copyrightable works.

A trademark holder may challenge a competitive use or registration of a similar domain name. The same applies to a copyright holder (although this is a more theoretical possibility, as the connection between copyright and domain is rather limited).

Law stated - 4 August 2026

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

The main legal framework is set in the [Advertising Act](#), which applies to both traditional offline and online advertising. Electronic communication as a form of commercial advertising is subject to additional anti-spam regulation set out in the E-Commerce Act. Online editorial content is also subject to additional sector-specific advertising rules of the Hungarian media regulation. The [Unfair Commercial Practice Act](#) sets out the rules against misleading advertising. The Hungarian Advertising Association is a self-regulatory organisation with its own [Code of Advertising Ethics](#).

Law stated - 4 August 2026

Targeted advertising and online behavioural advertising

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

The law does not define targeted advertising and online behavioural advertising, but it does define electronic communication. The Hungarian E-Commerce Act defines electronic communication broadly as any commercial ads or notices relating to social aims communicated via an information society service or electronic communication service. In general, an advertisement does not have to be strictly separated from online editorial content, but the advertisement must be clearly recognisable in the online content.

A prior notice about the electronic communication is required – this notice must highlight in a clear manner:

- the fact that it is an electronic communication;
- the advertiser; and
- promotional offers or games (if applicable).

Under the E-Commerce Act, consent for receiving electronic communication is required. However, the Data Protection Authority recognises electronic marketing communication based on opt-out possibility in the case of offering products to existing customers.

Law stated - 4 August 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

The rules of misleading online advertising are set out in the Unfair Commercial Practice Act. In principle, these rules apply centrally, but there are also some related industry-specific rules (eg, in the pharma and financial industries). The burden of proof depends on whether the supervisory authority examines the advertising based on the truthfulness of the information or the capability of the information to mislead consumers. In the former case, the business must prove that the information in the advertisement is correct.

Law stated - 4 August 2026

Restrictions

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

Hungarian advertising law has restrictions and bans (such as banning tobacco adverts and, under certain conditions, alcohol and gambling adverts); however, in principle, all products that may be advertised offline may be advertised online as well. An exception applies to reminder advertising of over-the-counter medicinal products or therapeutic medical devices

that are not supported by social security, and as such reminder advertising may not be carried out via the internet.

Law stated - 4 August 2026

Direct email marketing

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

In general, electronic marketing (via email, fax or SMS) is allowed only based on consent. However, the Data Protection Authority recognises electronic marketing communication based on opt-out possibility in the case of offering products to existing customers. Regarding voice-to-voice calls, the individual may be called only if he or she has not objected to such communication in the Hungarian publicly available phone directories (eg, no "S" sign or other mark in the directories, showing that the person cannot be called for marketing purposes). In case of automated calls, the holder of the phone number must give their prior explicit consent for the call (eg, in the phone subscription contract).

Law stated - 4 August 2026

ONLINE PUBLISHING

Hosting liability

22 | 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?

Both content providers and ISPs (host providers) can be liable for unlawful advertisements if they are qualified as a publisher of advertisements. A publisher of advertisements is an entity that has the technical means to publish the advertisements.

Content providers as publishers will be liable if they could have had knowledge of the nature of the content before publishing the advertisement.

ISPs as publishers will be liable only if they did not remove the unlawful advertisements forthwith upon becoming aware of their illegal nature. However, ISPs providing video-sharing services can be also liable if they do not comply with their obligation to filter out certain commercial communications.

Law stated - 4 August 2026

Content liability

23 | 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?

As a general rule, as long as the website provider is a content provider and not an ISP (such as a host, search engine or cache provider), it is liable for any of its own content made available on its site. This liability cannot be removed with a unilateral disclaimer notice. The website provider is also liable for third-party content, but it can avoid such liability under certain conditions (eg, it has a proper notice-takedown mechanism for inappropriate user comments, or it re-publishes defamatory content, but marking the source and allowing the possibility for the other party to react).

Law stated - 4 August 2026

Shutdown and takedown

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

It depends on the nature of the content. The ISP is not in a position to determine the truth of the allegation as it cannot take the role of judge. On the other hand, the truth defence is not relevant when, irrespective of whether the statement is correct or not, it unjustifiably breached the personal right of the person (eg, posts an offensive comment) and the ISP became aware of such statement. In this case, the content is 'manifestly unlawful' and the ISP must remove such content without further consideration.

Law stated - 4 August 2026

INTELLECTUAL PROPERTY

Data and databases

- 25** | Are data and databases protected by IP rights?

The database can be qualified as a copyrighted work if the selection, arrangement or editing of its content is of an individual and original nature. In this case, the website provider can protect its database based on regular copyright protection.

The website provider as the maker of the database also has sui generis rights. These rights apply if a substantial investment has been required to obtain, verify or present the content of the database. Based on sui generis rights, the website provider could also prevent the reproduction of its database.

Law stated - 4 August 2026

Third-party links and content

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

This must always be assessed on a case-by-case basis. In general, if the third-party website targeted all internet users and was not protected (eg, subject to a paywall), a link to a third-party website is permissible. Users shall always have the clear ability to identify the original source and to understand that the website owner merely links to a third-party website (without having any relationship with the third-party website). If the linked third-party website contains unauthorised content, the website owner may be also liable.

Law stated - 4 August 2026

- 27** | 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?

A website owner may only use third-party content on its website without permission if there is some specific permitted case of fair use (citation, free lecture, parody, orphan works, etc) to the extent it is used within the specific limits of fair use as set out in the [Copyright Act](#). Otherwise, the website owner's unauthorised use of third-party copyright work can constitute copyright infringement, and the potential consequences can be civil in nature as well as criminal.

Law stated - 4 August 2026

Metaverse and online platforms

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

Given its virtual nature, the metaverse presents numerous practical challenges for establishing or enforcing intellectual property (IP) rights in Hungary (as in other jurisdictions). These include how to apply copyright rules in a borderless digital environment, how to protect content in the absence of a clear takedown mechanism, and how to assess trademark similarity between real-world and virtual goods or services.

Hungary applies EU-level developments, including EUIPO's updated classification rules, which now allow trademark protection for 'virtual goods' and NFTs under the Nice Classification, provided the underlying digital content is clearly specified. However, other aspects of IP law remain uncertain. Copyright enforcement is hindered by the lack of intermediary liability frameworks for virtual platforms and user-generated content. Similarly, it is unclear whether sui generis database rights extend to the dynamic and decentralised data structures typical of metaverse environments.

The scope of IP protection in Hungary as it relates to the metaverse remains untested, and the Hungarian Intellectual Property Office has not yet issued any specific guidance.

Law stated - 4 August 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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?

Hungarian law recognises the first-sale doctrine. The Copyright Act states that if the copy of the work has been put into circulation within the European Economic Area by the copyright holder or another person (expressly authorised by the copyright holder), then the copyright holder's or authorised person's right to control the distribution shall later be exhausted with regard to that copy.

In general, the first-sale doctrine applies only to physical (tangible) products, not digital products.

However, the landmark decision of the European Court of Justice in [UsedSoft GmbH v Oracle International Corp](#) (Case No. C-128/11) strengthened the argument that if the copyright holder makes the software available for download on the internet for an appropriate fee, then the first-sale doctrine could apply to the software purchased by the person who downloaded it if, in the course of resale, it is ensured that the original copy does not remain with the licence holder/reseller. As Hungarian copyright law needs to be interpreted in line with EU copyright law, the conclusions of this decision could apply, mutatis mutandis, to Hungary. Nevertheless, subsequent CJEU case law has confirmed that this exception does not generally extend to other categories of digital content.

Law stated - 4 August 2026

Administrative enforcement

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

The Hungarian Tax and Customs Administration has jurisdiction when an IP infringement constitutes a criminal offence, and it can order dawn raids and freezing injunctions. In litigation civil courts can also order freezing injunctions.

In the online context, if the IP infringement constitutes a crime, the criminal court can order the online host provider to remove the unlawful content within one day.

Law stated - 4 August 2026

Civil remedies

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

Various civil remedies are available to IP owners via both final court decisions and interim injunctions, including:

- the right to claim damages;
- the right to request cessation of the infringement;
- the right to claim recovery for unjust enrichment of the infringer;
- the right to claim seizure or destruction of infringing goods;
- the right to request a public court order or a public statement with appropriate content and form;
- the right to request removal of the infringing goods from the market; and
- the right to request information about the parties involved in the performance of services affected by the infringement as well as about the business network established by the infringing acts.

Law stated - 4 August 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

- 32** | 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?

Personal data may be any data by which the individual can be directly or indirectly identifiable. Anonymisation techniques can be used to avoid Hungarian data protection regulation as long as the connection between the personal data and the individual is lost forever.

In the case of special categories of personal data (often referred to as sensitive data), such as health, biometric or political opinion data, controllers must demonstrate that a specific legal ground under article 9 GDPR is met, in addition to the general grounds under article 6.

Processing special category data also triggers heightened legal obligations, including: (1) greater risk of harm in the event of a data breach, (2) higher threshold for security measures and often (3) need to conduct a data protection impact assessment.

Law stated - 4 August 2026

Registration and appointment of data protection officer

- 33** | 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?

Parties involved in the processing of personal data are no longer required to register with the Hungarian data protection authority to process personal data; instead they shall maintain their internal records of processing in line with article 30 of the GDPR. However, the GDPR's notification obligations (such as data breach or data protection officer notification) are directly applicable in Hungary.

Law stated - 4 August 2026

Extraterritorial issues

- 34** | 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?

Hungarian data protection laws apply to organisations outside of Hungary if the data processing operation of such organisations relates to offering goods and services to individuals located in Hungary or to monitoring individuals' behaviour that occurs in Hungary. In this case, a foreign national who is residing in Hungary has the same protection under Hungarian data protection law as Hungarian citizens.

Law stated - 4 August 2026

Bases for processing

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

In the Hungarian digital world, apart from consent, performance of contract and legitimate interest are very common legal grounds for processing personal data.

Businesses may use performance of contract to the extent it is connected to the provision of service. In any other case, where the data processing operation is not directly connected to the provision of service (eg, improving a website or marketing), performance of contract is not the appropriate legal ground.

Businesses may also use legitimate interest, if they carry out and document the legitimate interest test in which they explain why the business's interest to process the data for a specific purpose overrides the right of privacy of customers. In the case of legitimate interest, the customer must be informed prior to the data processing that he or she has the right to object to it (eg, a proper opt-out mechanism must be ensured).

Consent is the primary legal ground in the case of electronic marketing. The consent must be informed (ie, the customer is properly informed about the data processing via a privacy policy), freely given (eg, if there are more data processing purposes a separate checkbox shall be provided for each data processing purpose) and explicit (eg, consent is not explicit if the checkbox is ticked by default).

In the case of transferring or exporting personal data to jurisdictions outside the European Economic Area, as a general rule, transfer or export is possible only if it is compliant with

adequate safeguards based on the General Data Protection Regulation and *Schrems II* decision (Case No. C-311/18) of the Court of Justice of the European Union.

Law stated - 4 August 2026

Data export and data sovereignty

- 36** | 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?

Under Hungary's Cybersecurity Act, effective from 1 January 2025, certain entities – including state bodies and critical infrastructure operators designated under national or EU law – are required to classify data before transferring it abroad or using public cloud services. The classification is based on the confidentiality, integrity and availability of the data, taking into account the potential material and reputational damage resulting from a security incident. Depending on the assigned classification level, data may be transferred without territorial restrictions, only within the European Union, or, for the highest-risk category, exclusively within Hungary.

Online betting servers must maintain their servers in Hungary, meaning that the data remain in Hungary as well.

Law stated - 4 August 2026

Sale of data to third parties

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

The Hungarian data protection authority is strict about the sale of data. The broker must inform the data subject that their data will be used for sale of data and the data subject must have the possibility to review the privacy policy of the database buyer and give consent to such transfer. This means that if there are several buyers, the data broker shall make available the privacy policy of each buyer, and ensure that data subjects can freely decide to which buyer their data can be transferred (eg, by checkbox mechanism).

On the other hand, the Hungarian data protection authority recognises the transfer of databases in M&A transactions based on legitimate interest of the seller.

Law stated - 4 August 2026

Consumer redress

- 38** | 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?

Individuals have the right to exercise rights set out in the GDPR, including the right to ask for information, access, erasure, restriction of processing, object to processing, data portability and not to be subject to automated decision-making (articles 13–22 GDPR). Individuals have the right to claim damages in the case of breach of their rights under the GDPR. These rights are equally granted to Hungarian citizens and foreign individuals to the extent the Hungarian data protection law applies.

Law stated - 4 August 2026

Non-personal data

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

Regulation (EU) 2018/1807 on the free flow of non-personal data applies directly; there is no specific national legislation on the use of non-personal data.

Law stated - 4 August 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

Certain legal transactions in family and inheritance law remain subject to mandatory formal requirements under Hungarian law, which may require paper-based documents, wet signatures or notarial involvement. Accordingly, fully electronic execution is not available in all cases.

Law stated - 4 August 2026

Retention

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

As a general rule, online contractual documentation subject to bookkeeping must be retained for eight years.

Law stated - 4 August 2026

DATA BREACH AND CYBERSECURITY

Security measures

.

- 42** | 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?

In general, companies and internet service providers are free to determine their own security measures, provided these comply with article 32 of the GDPR, which requires appropriate technical and organisational safeguards against data breaches. However, additional obligations apply to critical infrastructure operators, entities falling under the NIS2 Directive (Directive (EU) 2022/2555), and those covered by the CER Directive (Directive (EU) 2022/2557), as implemented by Hungary's Cybersecurity Act.

These entities are required to apply the security classification method set out in MK Decree 7/2024, which assigns an information system a risk level (Level 1, 2, or 3) based on its exposure and criticality. This classification is decisive in determining the appropriate security control measures, as the decree lists hundreds of specific controls that must be applied depending on the assigned level.

While Hungarian law does not explicitly require encryption for internet transactions, encryption is widely recommended to reduce the risk of personal data breaches. For high-risk entities under the Cybersecurity Act, encryption and other technical controls may become mandatory based on the classification outcome.

Law stated - 4 August 2026

Data breach notification

- 43** | 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?

The provisions of the GDPR on data breach notification and data security are directly applicable, but there are also some sector-specific Hungarian laws.

Electronic communication service providers must notify the data breach to the Hungarian Media and Infocommunications Authority (first notification within 24 hours, second notification within 72 hours after obtaining knowledge about the breach).

Hungary has also implemented the NIS2 Directive (EU Directive No. 2022/2555), based on which certain organisations falling under the scope of the NIS2 Directive must report security breaches (including data breaches) that have a significant impact on the provision of their services.

Law stated - 4 August 2026

Government interception

- 44** | 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?

Hungarian law enforcement authorities usually access electronic communication via data disclosure requests. Some law enforcement authorities (such as the police and national security) may also intercept the content of communication carried out by means of electronic communications networks or devices or any information system under certain conditions.

Law stated - 4 August 2026

GAMING

Legality and regulation

45 | 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?

It depends on the type of gambling:

- Online betting is permissible, but a licence for operating is required. Hungarian incorporation is also required (for EEA applicants, having a Hungarian branch is sufficient).
- Lotteries may not be performed (as raffles may not be performed online, and other lottery games are subject to state monopoly).
- Online casinos may be organised only by the entity that has the concession right to run casinos in Hungary as brick-and-mortar premises.

Law stated - 4 August 2026

Cross-border gaming

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

It is permissible to advertise or provide access to online gambling business if the business has a valid licence for operation.

Most gambling activities require a Hungarian licence, and many times those licences are given to companies that have state monopoly (or concession right). The only liberalised field is online betting. Namely based on the ECJ decision C-3/17, Hungary has liberalised remote gambling. This means that EEA-based gambling operators may also apply for online betting. However, this is far from full liberalisation as such gambling operators need to establish a Hungarian branch, obtain a Hungarian licence (remote foreign licences are not recognised) and pursue the activity from Hungarian servers only.

Law stated - 4 August 2026

OUTSOURCING

Key legal issues

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

The contract rules of the Hungarian Civil Code set the general framework for outsourcing. In some specific industries such as financial or energy) sector-specific outsourcing rules also apply. Outsourcing also raises important employment issues especially in respect of control rights and transfer of employees. Taxation is also an important aspect of outsourcing deals as it needs to be checked whether the outsourcing transaction is subject to taxation. In the case of involvement of low-cost jurisdictions, anti-avoidance rules shall be also taken into account.

Law stated - 4 August 2026

Sector-specific issues

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

As a general rule, there are no digital business services that cannot be outsourced. However, if the digital businesses fall within specific industries (such as the financial or energy industries), outsourcing is possible only if the requirements of the sector-specific legislation are observed.

Law stated - 4 August 2026

Contractual terms

- 49** | Does the law require any particular terms to be included in outsourcing contracts?

Outsourcing contracts must incorporate the data processing agreement elements required under article 28 of the GDPR. Where the outsourcing involves cloud computing, it is also advisable to follow established EU data protection best practices, such as those set out in WP29 Opinion 05/2012 on Cloud Computing and the Sopot Memorandum, which remain influential despite their age.

For entities in the financial sector, outsourcing agreements are additionally subject to sector-specific regulatory requirements. In particular, contracts should reflect the expectations set out in the EBA Guidelines on Outsourcing Arrangements. The Central Bank of Hungary (MNB) has acknowledged these guidelines in its Recommendation 7/2020, which includes provisions on audit rights, termination rights, and other key contractual elements. While not all EBA requirements are fully mirrored, the MNB's approach reinforces the importance of aligning outsourcing arrangements with EU-level standards, particularly where critical or ICT-related functions are involved.

Law stated - 4 August 2026

Employee rights

- 50** | 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?

In general, in the case of business transfers, the employment relationship is transferred to the transferee. Employment terms (including salary) remain unchanged at the time of the transfer. The transferee must maintain the collective agreement's terms for one year. The transferee may suggest amendments of the terms, but the employee may refuse such suggestions and the employer may not terminate the agreement based on such refusal. Prior consultation with a works council and employee notification is also a mandatory part of the process.

Law stated - 4 August 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

The EU AI Act is directly applicable in Hungary and is being introduced in phases. Hungary has also designated the competent authorities responsible for the supervision and enforcement of the AI Act.

The Act adopts a risk-based approach: AI practices posing unacceptable risks are prohibited; high-risk AI systems (eg, AI used in recruitment or creditworthiness assessment) are subject to extensive risk management, governance, documentation, transparency and human oversight requirements; certain AI systems, such as chatbots and AI systems generating synthetic content, are subject to transparency obligations; while AI systems not falling within these categories remain largely unregulated under the AI Act, apart from voluntary codes of conduct.

Where AI involves the processing of personal data, compliance with the GDPR remains essential. Although a data protection impact assessment (DPIA) is not automatically required merely because AI is used, it will frequently be necessary where the processing is likely to result in a high risk to individuals' rights and freedoms, particularly in cases involving profiling, automated decision-making, large-scale processing, sensitive personal data or vulnerable data subjects.

In February 2022, the Hungarian Data Protection Authority imposed a record GDPR fine (250 million forints) on a bank for its automatic AI analysis of customer service call recordings. Among other findings, the authority held that the bank had failed to demonstrate the proportionality of the processing and had not provided meaningful information to data

subjects. The decision remains an important benchmark for AI deployments involving personal data.

Law stated - 4 August 2026

IP rights

- 52** | 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?

Hungarian law does not yet regulate intellectual property (IP) generated by artificial intelligence. Under current rules, only natural persons can be authors or inventors, meaning AI-generated works are not eligible for copyright or patent protection. If AI is merely used as a tool and the human retains creative control, copyright or patent protection may still apply. In addition, AI-related assets such as training datasets, model parameters, prompts or fine-tuning methodologies may also be protected as trade secrets where the statutory requirements are met.

AI-generated names or logos may be registered as trademarks if they are distinctive and do not conflict with existing marks. However, if the AI-generated sign is not reviewed by a human, it may be rejected for lacking distinctiveness or for resembling earlier trademarks. A prior trademark search is recommended.

There is no standalone IP regime governing AI training data, but datasets may be protected under copyright, sui generis database rights, or contractual terms, depending on their content and structure.

Overall, ownership and reuse of training data therefore depend on the nature of the dataset, its structure, and any third-party rights involved.

Law stated - 4 August 2026

Ethics

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

No local rules or guidance relating to the ethics of artificial intelligence and machine learning have been issued.

Law stated - 4 August 2026

TAXATION

Online sales

.

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

In general, distance sales of goods are subject to Hungarian VAT where the goods are delivered to consumers in Hungary. Digital services are generally subject to Hungarian VAT where, under the applicable VAT rules, the place of supply is Hungary.

For cross-border B2C supplies within the EU, VAT is generally payable in the Member State where the goods are delivered or, in the case of digital services, where the place of supply is deemed to be located. An exception applies to certain suppliers whose annual cross-border B2C supplies do not exceed the EU-wide threshold of €10,000. Businesses may generally use the optional One Stop Shop (OSS) scheme to declare and pay VAT due in other Member States.

Law stated - 4 August 2026

Server placement

55 | 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?

If the company is incorporated outside of Hungary and its place of management is not in Hungary, the company will not be a Hungarian tax resident. However, the company can be still subject to Hungarian corporate tax on income earned in Hungary if the server is placed within Hungary and the company carries out its business activity in Hungary in whole or in part through that server. Hungarian VAT can apply under certain conditions (eg, the place of supply is in Hungary) irrespective of where the servers are located.

Law stated - 4 August 2026

Electronic invoicing

56 | 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?

In Hungary, businesses must provide copies of e-invoices to the tax authority. Simultaneously, they must report invoicing data electronically in XML format to the tax authority. These notifications are made to the tax authority's [online invoice system interface](#).

Law stated - 4 August 2026

DISPUTE RESOLUTION

Venues

|

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

There are no special courts or other venues in Hungary that specifically deal with online/digital issues and disputes.

Law stated - 4 August 2026

ADR

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

The most common ADR form is the proceeding before the [Hungarian conciliation body](#).

Businesses must inform consumers about the possibility of initiating conciliation proceedings. While participation in the procedure is mandatory for businesses, they are not generally obliged to accept a settlement or be bound by the outcome.

The former EU Online Dispute Resolution (ODR) Platform established under Regulation (EU) No 524/2013 was discontinued in 2025. Cross-border online consumer disputes are therefore resolved through the ordinary ADR mechanisms available under national law, including the Hungarian consumer conciliation body, or before the competent courts.

Law stated - 4 August 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

The Hungarian digital regulatory landscape has undergone significant transformation in recent years, driven primarily by new EU digital legislation and its national implementation.

- **Artificial intelligence:** The EU AI Act has introduced the world's first comprehensive legal framework for AI, with its obligations becoming applicable in phases. Hungary has also designated the competent authorities responsible for its supervision and enforcement.
- **Data economy:** The EU Data Act has established a new framework for B2B and B2C data sharing, aiming to facilitate access to and reuse of connected product and related service data.
- **Cybersecurity:** Hungary has implemented the NIS2 Directive through a new Cybersecurity Act, significantly expanding the number of regulated organisations. Depending on the security classification of their information systems, organisations

may be required to implement approximately 160–380 cybersecurity measures. The new framework also introduced data classification requirements that may result in territorial restrictions on certain cross-border data processing activities.

- Financial services: The financial sector continues to experience significant regulatory change through measures such as MiCA, DORA and the forthcoming PSD3 reform package.
- Digital identity: Hungary has introduced a new digital identity framework, including the Digital Citizenship Programme and digital wallet solutions, in line with broader European developments.
- Consumer protection and online platforms: The implementation of the Digital Content Directives and the Omnibus Directive has strengthened consumer protection in the digital environment, while the Digital Services Act has further expanded the regulatory obligations of online intermediaries and platforms.

Law stated - 4 August 2026



Endre Várady
János Tamás Varga

varadye@vjt-partners.com
vargajt@vjt-partners.com

VJT & Partners

[Read more from this firm on Lexology](#)

India

[Hardeep Sachdeva](#), [Priyamvada Shenoy](#), [Shagun Badhwar](#), [Nishant Thakur](#),
[Sahil Tandon](#), [Amulya Bhatia](#)

[AZB & Partners](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

India adopts a multi-stakeholder approach to digital regulation, recognising the role of government, industry, and other relevant stakeholders in the development of digital laws and regulatory frameworks. This approach is reflected in consultations on key legislative and regulatory initiatives, including the Digital Personal Data Protection Act, the proposed Digital India Act, and AI governance. By engaging stakeholders throughout the regulatory process, India seeks to develop balanced frameworks that support innovation, enhance legal certainty, and protect public interests, while reaffirming its longstanding support for the multi-stakeholder model of internet governance in both domestic and international forums.

While stakeholder consultation is a common feature of India's digital regulatory framework, the extent of consultation has varied across legislative and regulatory initiatives.

Law stated - 8 September 2026

Legislation

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

The Information Technology Act, 2000 (IT Act), read with the rules and regulations framed thereunder, is the principal legislation regulating the digital space in India. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication but also contains provisions that are aimed at safeguarding electronic data, information and records, and preventing unauthorised or unlawful use of a computer system.

Some of the relevant rules framed under the IT Act that regulate and govern digital content and businesses include the following:

- the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for the collection and processing of personal or sensitive personal data;
- the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, which require specific information security measures to be implemented by organisations that have protected systems, as defined under the IT Act; and
- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), which require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein in terms of the SPDI Rules, and which have been

substantially amended with effect from February 20, 2026 to introduce a dedicated compliance framework for synthetically generated information, including labelling and provenance requirements for content generated using artificial intelligence.

The Promotion and Regulation of Online Gaming Act, 2025 is the principal central legislation governing online gaming in India. Prior to its enactment, online money gaming was not subject to a dedicated central statutory framework and was regulated primarily under state gaming and gambling laws, which varied across jurisdictions and, in several States, distinguished between games of skill and games of chance, permitting certain real-money skill-based games subject to applicable licensing and regulatory requirements. The Act establishes a uniform national framework by prohibiting all forms of online money gaming, irrespective of whether the underlying game is one of skill, chance, or a combination of both. It applies throughout India and has extraterritorial effect, extending to online money gaming services operated from outside India where such services are offered or made available to persons in India.

Other laws including the Bharatiya Nyaya Sanhita, 2023 (BNS) (replacing the earlier Indian Penal Code, 1860), also provide for specific offences, including those committed in cyberspace (such as defamation, cheating and criminal intimidation), and the Companies (Management and Administration) Rules, 2014, framed under the Companies Act, 2013, which require companies to ensure that their electronic records and security systems are secure from unauthorised access and tampering. There are also sector-specific regulations issued by regulators such as the Reserve Bank of India, the Insurance Regulatory and Development Authority of India (constituted under the Insurance Regulatory and Development Authority Act, 1999), the Department of Telecommunications and the Securities and Exchange Board of India, which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities.

In addition to the above, India has overhauled its data protection regime under the Digital Personal Data Protection Act, 2023 (DPDP Act), which is being operationalised through a staggered implementation framework. The Digital Personal Data Protection Rules, 2025 (DPDP Rules) were notified and published in the Official Gazette on 13 November 2025. Sections 18 to 26 of the Digital Personal Data Protection Act, 2023, together with Rules 1, 2 and 17 to 21 of the Digital Personal Data Protection Rules, 2025, came into force on 13 November 2025. Rule 4, relating to the registration and obligations of Consent Managers, will come into force on 13 November 2026. The substantive provisions of the Act and Rules—including those governing notice and consent, data principal rights, processing of children's personal data, security safeguards, personal data breach notification, cross-border data transfers and enforcement (comprising Rule 3, Rules 5 to 16 and Rules 22 and 23)—will come into force on 13 May 2027. Once fully in effect, the DPDP Act read with the DPDP Rules will introduce a comprehensive and uniform framework governing the processing of personal data by all data fiduciaries, including foreign entities processing personal data of individuals located in India, and will require compliance with principles such as lawful processing, purpose limitation, data minimisation, consent standards and accountability.

With the introduction of the DPDP Act and the DPDP Rules, Section 43A of the IT Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 will be superseded entirely. While the

erstwhile regime under the IT Act and SPDI Rules prescribe compliance with the ISO standards, Rule 6 of the DPDP Rules, instead of prescribing any standards, lays down the standards for "reasonable security safeguards", which includes appropriate data security measures, such as through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data, appropriate measures to control access, and also requires appropriate measures for ensuring detection, investigation and remediation of instances of unauthorised access.

The DPDP Act provides for substantial financial penalties. The highest penalty, of up to 2.5 billion rupees (approximately US\$29 million), may be imposed for a failure by a data fiduciary to implement reasonable security safeguards to prevent a personal data breach. A failure to notify the Data Protection Board and affected data principals of a personal data breach, and a contravention of the additional obligations relating to children's personal data, each attract penalties of up to 2 billion rupees (approximately US\$23 million). A Significant Data Fiduciary that breaches its additional statutory obligations may be subject to a penalty of up to 1.5 billion rupees (approximately US\$17 million). Any other contravention of the DPDP Act or the DPDP Rules by a data fiduciary may attract a penalty of up to 500 million rupees (approximately US\$5.8 million).

Law stated - 8 September 2026

Regulatory bodies

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

There are several relevant government agencies responsible for the regulation of e-commerce, data protection and internet access tariffs and charges, etc.

The Department for Promotion of Industry and Internal Trade (DPIIT) regulates foreign direct investment (FDI) in e-commerce. The Press Note No. 2 dated December 12, 2018, issued by the DPIIT (PN2) sets out the settled framework for FDI concerning the e-commerce sector.

Further, the Ministry of Consumer Affairs, Food and Public Distribution has notified the Consumer Protection Act, 2019 (CPA 2019) and the Consumer Protection (E-Commerce) Rules 2020 (E-Commerce Rules). The term 'consumer' is defined under the CPA 2019 as any person who buys goods or services for consideration but excludes any person who makes a purchase for "commercial use", with the exception of goods bought for the purpose of earning livelihood by means of self-employment. The CPA 2019 addresses issues in respect of digitisation and e-commerce. The E-Commerce Rules, formulated under the CPA 2019, regulate e-commerce entities and provide a framework to regulate the marketing, sale and purchase of goods and services online provided by such e-commerce entities. The E-Commerce Rules also apply to entities that are not established in India but systematically offer goods or services to consumers in India. The Central Consumer Protection Authority (set up under the CPA 2019) regulates matters relating to violation of rights of consumers, unfair trade practices and false or misleading advertisements which

are prejudicial to the interests of public and consumers and to promote, protect and enforce the rights of consumers as a class.

The IRDAI has separately notified the IRDAI (Bima Sugam - Insurance Electronic Marketplace) Regulations, 2024, allowing the establishment of a Digital Public Infrastructure called Bima Sugam - Insurance Electronic Marketplace to facilitate, among other matters, the purchase, sale and servicing of insurance policies and the settlement of claims.

The payment systems for online e-commerce transactions, and the usage of payment instruments for facilitating e-commerce and mobile commerce are regulated by the Reserve Bank of India (RBI). RBI has also issued Foreign Exchange Management (Transfer or Issue of Security by a Person Resident outside India) (Amendment) Regulations 2019 dated 1 February 2019, to make it consistent with the revised legal framework stipulated under PN2.

Ministry of Electronics and Information Technology (MeitY) together with the Ministry of Communications (MoC) has been entrusted to promote the internet, IT and e-commerce in India. Under MeitY, the Computer Emergency Response Team (CERT-In) has been established as the nodal agency to respond to cybersecurity incidents, and to undertake emergency measures in relation to such cybersecurity incidents. At the same time, the RBI regulates payment systems and online e-commerce transactions.

Telecom service providers in the country (including ISPs) are licensed by the Department of Telecommunications (DoT) under the MoC. Further, in accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, CERT-In has been established as the nodal agency which is responsible for the collection, analysis and dissemination of information on cyber incidents and taking emergency measures to contain such incidents. The access charges and tariffs in relation to the aforementioned service providers are regulated under their license from the DoT and the tariff orders and regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time.

TRAI has been established to regulate telecom services, including the fixing or revision of tariffs for telecom services that were earlier vested with the central government. One of the main objectives of TRAI is to provide a fair and transparent policy environment that promotes a level playing field and facilitates fair competition. The directions, orders and regulations issued cover a wide range of subjects including tariffs, interconnection and quality of service.

The Competition Commission of India (CCI) is responsible for enforcing competition law in digital markets. In addition, the Committee on Digital Competition Law recommended the introduction of an ex-ante regulatory framework for designated Systemically Significant Digital Enterprises through a proposed Digital Competition Bill, 2024. However, the Bill has not been introduced in Parliament or enacted, and the CCI currently continues to regulate digital markets under the Competition Act, 2002. In a significant development for India's digital payments ecosystem, the RBI established the Payments Regulatory Board (PRB) through a notification dated May 20, 2025. The PRB has been constituted as a specialised regulatory body to oversee and regulate payment systems in India, with the objective of ensuring the safety, efficiency, and innovation in the payments landscape. The PRB is empowered to formulate policies, issue guidelines, and take regulatory decisions related to

payment systems, digital payments, and fintech innovations. This establishment represents a major step towards strengthening the regulatory framework for India's rapidly evolving digital payments sector and aligns with the government's vision of promoting a cashless economy and financial inclusion.

The Data Protection Board of India (DPBI) has been established under Section 18 of the Digital Personal Data Protection Act, 2023 as an independent adjudicatory body corporate. The provisions establishing the DPBI came into force on 13 November 2025. The DPBI is responsible for inquiring into personal data breaches and other instances of non-compliance with the DPDP Act, issuing directions for mitigation and remediation, imposing monetary penalties, and otherwise enforcing the Act. It comprises a Chairperson and Members appointed by the Central Government, with its head office located in the National Capital Region.

Law stated - 8 September 2026

Jurisdiction

- 4 | 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?

In view of judicial precedents, cause of action is the key element in determining the jurisdiction by Indian courts. The Indian courts have jurisdiction to adjudicate where the cause of action arises in India, even where the goods and services are being provided from outside the country.

Where a defendant sells goods or provides services from outside India, it has been seen that the Indian courts have exercised jurisdiction and adjudicated cases involving deficiency in goods or services under the Indian consumer protection laws. Now, the Consumer Protection (E-Commerce) Rules, 2020 (E-Commerce Rules) specifically recognise and apply to entities that are not established in India but systematically offer goods or services to consumers in India such as offshore online marketplaces. Accordingly, courts may exercise jurisdiction where the E-Commerce Rules apply to offshore entities, however, jurisprudence in this space is still evolving. On the other hand, if services are provided by resident entities, it may be stated that the appropriate Indian courts will exercise jurisdiction. As a matter of public policy, Indian courts may not permit their jurisdiction to be ousted in a contract between an Indian service provider and service recipient. If, however, the service provider is not from the territorial boundaries of India, then in such a case, the E-Commerce Rules contemplate extraterritorial jurisdiction.

Law stated - 8 September 2026

Establishing a business

- 5 | 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?

Digital businesses in India are subject to a complex regulatory framework that includes compliance primarily with the Information Technology Act, 2000 and the rules and regulations made thereunder. In addition, digital businesses must comply with specific consumer protection rules established under the Consumer Protection (E-Commerce) Rules, 2020, which amongst others, prohibit unfair trade practices.

Selling digital content and services requires secure payment systems, compliance with the Payment and Settlement Systems Act, 2007 and, where applicable, adhering to rules for cross-border transactions, including provisions of the Foreign Exchange Management Act, 1999 and the rules and regulations made thereunder. Digital businesses must also ensure that they follow guidelines for data storage and protection, cybersecurity, and ensure they remain up to date with the requirements for secure online operations. This emphasis on digital compliance and consumer data protection distinguishes digital platforms from traditional setups.

Compared to brick-and-mortar businesses, many procedural requirements for digital operations, such as data privacy obligations and online consumer protection, may be more stringent and require greater compliance. While both types of businesses are subject to general commercial laws and taxation, digital enterprises face unique obligations such as registration and compliance in respect of online information and database access or retrieval services under the goods and services tax regime, implementing robust cybersecurity measures, and adhering to ever-evolving regulations designed specifically for online transactions. Overall, the establishment process for digital businesses is relatively seamless, but it comes with additional regulatory responsibilities reflective of India's rapidly growing digital market.

Law stated - 8 September 2026

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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, it is possible to form and conclude contracts electronically in terms of Section 10-A of the Information Technology Act, 2000 (IT Act). As long as the essentials of a valid contract under the Indian Contract Act, 1872 are met, an online contract is valid and enforceable under Indian law. The IT Act provides validity to a contract where the contract has been accepted in electronic form.

Additionally, the Bharatiya Sakshya Adhiniyam, 2023 (replacing the earlier Indian Evidence Act, 1872) governs admissibility of electronic records and contracts, and states that any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer will be deemed a document of proof and will be admissible in any proceedings, without further proof or production of the original, subject to satisfaction of the conditions prescribed under the Bharatiya Sakshya Adhiniyam, 2023.

Law stated - 8 September 2026

Applicable laws

- 7 | 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?

There are no particular laws that limit the choice of governing law, language of the contract or forum specifically for disputes arising from digital contracts. These questions are often decided in accordance with customary practice and the settled legal position, depending on the specific facts and circumstances surrounding the dispute. In the context of arbitrations, the same is left to determination of the parties, and courts generally give effect to such choice of law clauses. This position is regardless of whether the dispute arises from a traditionally executed contract or from a digital contract.

Law stated - 8 September 2026

Electronic signatures

- 8 | 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?

The Information Technology Act, 2000 (IT Act) provides legal recognition to electronic signatures and lays down the framework that governs their use. It expressly includes 'digital signature' as a form of electronic signature, subject to its adherence to the authentication requirements prescribed under the IT Act. An electronic signature may be used at any place where any law provides for the use of a signature for authentication. An 'electronic signature' refers to the authentication of an electronic record by a subscriber by means of the prescribed electronic technique and includes digital signatures. Usage of digital signature is very common for e-filing of statutory forms with the Ministry of Corporate Affairs, and goods and services tax authorities.

As per the IT Act read with the Information Technology (Certifying Authorities) Rules, 2000, an entity proposing to issue digital signatures (as recognised under the law) requires a licence, namely, a digital signature certificate from the Controller of Certifying Authorities. While the IT Act recognises electronic signatures, only an electronic contract with a digital signature certified in accordance with the IT Act and the rules thereunder attracts statutory presumptions which materially ease proof of the integrity and authenticity of an electronic contract.

Law stated - 8 September 2026

Breach

- 9 |

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

The remedies available under the Indian Contract Act, 1872 for breach of a contract may also be availed for electronic contracts. There are no specific remedies or designated forums for dispute resolution prescribed for the breach of an electronic contract in India.

Law stated - 8 September 2026

FINANCIAL SERVICES

Regulation

10 | 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?

The digital advertising and sale of financial services in India is subject to a regulatory framework designed to protect consumers, prevent false or misleading advertising, and ensure market integrity, and is overseen by several key regulatory authorities, depending on the type of financial product being promoted or the nature of the advertising entity. These regulators include the Reserve Bank of India (RBI) for banking and digital lending, the Securities and Exchange Board of India (SEBI) for investment and advisory services and the Insurance Regulatory and Development Authority of India (IRDAI) for insurance products.

Sectoral regulators have issued specific requirements governing the digital distribution and marketing of financial products. In the digital lending sector, the RBI has established a comprehensive regulatory framework governing regulated entities, lending service providers and digital lending applications. The framework, initially set out in the Reserve Bank of India (Digital Lending) Directions, 2025, has subsequently been incorporated into the digital lending chapters of the RBI's entity-specific Credit Facilities Directions, 2025 issued for different categories of regulated entities. These requirements address customer protection, disclosures, data governance, grievance redressal, and the conduct of regulated entities and their lending service providers.

The RBI framework requires regulated entities to provide borrowers with prescribed disclosures, including a Key Fact Statement, and imposes transparency requirements where digital platforms facilitate offers from multiple lenders. The RBI has also introduced reporting requirements for digital lending applications used by regulated entities to strengthen regulatory oversight of digital lending activities.

In the securities market, SEBI's regulations require investment advisers and mutual fund distributors to include risk disclaimers, avoid return guarantees, and refrain from associating with unregistered "financial influencers".

SEBI has issued regulatory measures restricting SEBI-regulated entities and their representatives from associating, directly or indirectly, with persons who provide securities-related advice or recommendations without being registered with or otherwise permitted by SEBI, or who make explicit or implicit claims regarding returns or performance of securities without appropriate regulatory authorisation. These measures

are intended to strengthen investor protection and address misleading digital promotion of securities-related services.

In the insurance sector, the IRDAI (Protection of Policyholders' Interests, Operations and Allied Matters of Insurers) Regulations, 2024, together with the relevant Master Circulars on Operations and Allied Matters of Insurers and Protection of Policyholders' Interests, have consolidated the framework governing insurance advertisements. The regulatory approach has moved towards greater board-level accountability and self-governance, with insurers required to establish internal advertisement approval mechanisms and ensure compliance with applicable disclosure and conduct requirements. Insurers are no longer subject to routine prior filing of advertisements with IRDAI, although IRDAI retains supervisory oversight. Unit-linked and index-linked insurance products must not be marketed or presented as investment products.

Non-compliance with these rules, regulations and frameworks can lead to significant penalties, including fines, suspension of licences, and legal risks. Regulatory bodies like SEBI and RBI have the authority to impose penalties for breaches, which can include monetary fines and suspension of operations.

The Advertising Standards Council of India (ASCI), a self-regulatory body, plays a key role in overseeing the content and ethical standards of digital advertising. ASCI has established the Code for Self-Regulation in Advertising (ASCI Code), designed to be followed in conjunction with existing legal frameworks. The Code complements statutory provisions and common law without overriding them. Its authority is further strengthened by Rule 7(9) of the Cable Television Networks Rules, 1994, which effectively makes adherence to the ASCI Code mandatory for broadcast advertisements. Consequently, any advertisement that violates the ASCI Code is prohibited from being aired on cable television.

Law stated - 8 September 2026

Electronic money and digital assets

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

The Constitution of India recognises that the Central Government, ie, the Government of India, has the exclusive power to make laws on subject matters enumerated under the Union List which includes "*currency, coinage and legal tender; foreign exchange*". While the term "*legal tender*" is not expressly defined under the Constitution of India or any central legislation, it is commonly understood to refer to currency, ie, bills and coins, officially recognised for the settlement of debts and transactions. The authority to legislate and regulate the issuance and use of such legal tender in India rests exclusively with the Central Government. Accordingly, various legislations have been enacted over time to regulate issuance of currency, coins, and legal tender, including particularly the Coinage Act, 2011 and the Reserve Bank of India Act, 1934.

India's regulatory landscape for electronic money, digital assets, and digital currencies is evolving rapidly, reflecting the country's cautious yet progressive approach to digital finance. The Reserve Bank of India (RBI) has been instrumental in shaping this framework,

particularly with the introduction of the Digital Rupee, India's Central Bank Digital Currency, in December 2022. This initiative aims to enhance financial inclusion, reduce currency printing costs, and facilitate real-time transactions. The Digital Rupee is designed to function as legal tender, offering secure and efficient payment solutions without the need for intermediaries like banks.

Compliance with anti-money laundering and counter-terrorism financing regulations is a critical consideration for entities dealing in digital currencies in India. The Prevention of Money Laundering Act, 2002, mandates that Virtual Digital Asset service providers register with the Financial Intelligence Unit – India (FIU-IND) and adhere to stringent KYC norms. This includes maintaining transaction records and reporting suspicious activities.

Additionally, in January 2026, FIU-IND issued the AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, 2026 (Guidelines), which consolidate and significantly enhance the compliance framework applicable to virtual digital asset service providers. The Guidelines codify the registration framework with FIU-IND, mandate the appointment of an India-based Principal Officer and a Designated Director with clearly delineated responsibilities, and require Board-level oversight of AML/CFT compliance. They also introduce a more prescriptive customer due diligence regime, including the collection of technical identifiers (such as IP addresses, geo-location data, wallet addresses and transaction hashes), tighter periodic KYC update timelines, enhanced transaction monitoring systems, travel rule implementation, and strengthened record-keeping and audit requirements, reflecting a clear shift towards implementation-driven and technology-enabled supervision of digital asset activities in India.

Further, payment and settlement systems in India are governed by the Payment and Settlement Systems Act, 2007 (PSS Act), read with the Payment and Settlement System Regulations, 2008. In terms of the PSS Act, the commencement or operation of a payment system in India shall be subject to authorisation by the RBI.

Notwithstanding these developments, India still has no dedicated regulatory statute governing crypto-assets. The applicable regime remains a composite of direct tax law, anti-money laundering obligations under the PMLA and the FIU-IND Guidelines, and, where a payment system is involved, authorisation under the PSS Act.

Law stated - 8 September 2026

Digital and crypto wallets

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

Presently, India does not have a dedicated law for regulating cryptocurrencies and crypto wallets.

The Prevention of Money-laundering Act, 2002 (PMLA) is the central legislation of India that deals with measures and safeguards against money laundering activities. On 7 March 2023, the Ministry of Finance through a notification brought the following activities within the purview of the PMLA:

- exchanging Virtual Digital Assets (VDAs) with fiat currencies;
- exchanging one VDA with another VDA;
- transferring VDAs between two persons or legal entities;
- safekeeping or administering VDAs or instruments enabling control over VDAs; and
- participating in and providing financial services related to the offer and sale of VDAs.

For dealing in VDAs, persons carrying on such activities are now required to register themselves with the Financial Intelligence Unit – India (FIU-IND) and undertake necessary compliances, disclosures and reporting requirements to the authorities to aid measures to prevent money laundering, in due compliance with the provisions of the PMLA.

Further, in January 2026, FIU-IND issued the AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets, 2026 (Guidelines), which are directly relevant for custodial crypto wallet providers and entities involved in the safekeeping or administration of VDAs. The Guidelines require FIU registration, enhanced KYC and transaction monitoring (including wallet addresses and transaction details), and impose restrictions on high-risk wallet features such as anonymity-enhancing tokens, mixers and certain unhosted wallet transactions, thereby placing practical compliance constraints on the operation of crypto wallets in India.

Separately, in April 2022, the Computer Emergency Response Team (CERT-In) issued certain directions to service providers, intermediaries, bodies corporate, virtual digital asset service providers, virtual asset exchange providers, custodian wallet providers, etc, mandating reporting of certain specified cyber incidents to CERT-In within six hours of noticing such incidents, and maintaining and retaining logs of all their information and communications technology systems for a rolling period of 180 days within India.

Separately, the Master Directions on Prepaid Payment Instruments have been issued by the Reserve Bank of India for prepaid payment instruments (PPIs) (eg, cards and wallets), regulating payment instruments that facilitate the purchase of goods and services against the value stored on such instruments. The issuers of PPIs are required to obtain a prior approval / authorisation from the RBI to set up/operate payment systems, under the Payment and Settlement Systems Act, 2007.

Further, the Finance Budget 2022 discussed aspects relating to the transfer of cryptocurrency in India and taxation on the income arising therefrom. Pursuant to the budget, the Indian Ministry of Law and Justice notified the Finance Act, 2022, which amended various provisions of the Income-tax Act, 1961 (ITA 1961), in order to, inter alia, introduce the concept of VDAs and taxation on the income arising from the transfer of such asset. India's direct tax code has since changed. The Income-tax Act, 2025 (ITA 2025) received Presidential assent on 21 August 2025 and came into force on 1 April 2026, replacing the ITA 1961, which continues to govern tax years beginning before that date. Accordingly, for financial year 2025-26 the ITA 1961 applies, and for financial year 2026-27 onwards the ITA 2025 applies. The provisions summarised below should be read together with their renumbered counterparts under the ITA 2025, in which sections are numbered sequentially and the total number of sections has been reduced.

As per the ITA 1961 (as amended by the Finance Act, 2022), the term 'virtual digital asset' has been defined to include, inter alia, any information, code, number or token (not being

Indian currency or foreign currency) generated through cryptographic means or otherwise, by whatever name called, that provides a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or that functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment schemes, and that can be transferred, stored or traded electronically.

As per Section 194S of the ITA 1961, any person responsible for paying to any Indian resident, any sum by way of consideration for transfer of a VDA, is required to deduct 1 per cent of such sum as income-tax thereon and deposit the same with government. However, no tax is required to be deducted where:

1. The consideration is payable by a 'specified person' and the value or aggregate value of such consideration does not exceed 50,000 Indian rupees during the financial year; or
2. The consideration is payable by any person other than a 'specified person' and the value or aggregate value of such consideration does not exceed 10,000 Indian rupees during the financial year.

As per Explanation to Section 194S of the ITA 1961, 'specified person' means (1) an individual or a Hindu undivided family, whose total sales, gross receipts or turnover from the business carried on by him or profession exercised by him does not exceed 10,000,000 Indian rupees in case of business or 5,000,000 Indian rupees in case of profession, during the financial year immediately preceding the financial year in which such VDA is transferred or (2) an individual or a Hindu undivided family, not having any income under the head 'profits and gains of business or profession'.

The substantive treatment of virtual digital assets is broadly preserved under the ITA 2025. Virtual digital assets are specifically recognised as capital assets for taxation purposes, and gains continue to be taxed at 30 per cent without any option to set off losses. Separately, Schedule VDA in the income tax return requires transaction-wise disclosure of every transfer of a virtual digital asset during the financial year, including the date of acquisition, the date of transfer, the head under which the income is taxed, the cost of acquisition, with specific rules where the asset was received as a gift, and the consideration received, a loss being reported as nil.

Law stated - 8 September 2026

Electronic payment systems

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

In India, the payment and settlement systems are regulated by the Payment and Settlement Systems Act, 2007 (PSS Act). Under the PSS Act, a 'payment system' is defined to mean a system that enables payments to be effected between a payer and a beneficiary and involves clearing, payment or settlement services, or all of them.

The nodal authority for regulating electronic payment systems, including payment aggregation activities, is the Reserve Bank of India (RBI). The RBI has issued the Master Direction on Regulation of Payment Aggregators, 2025 (PA Directions) on September 15, 2025, which consolidates and supersedes earlier guidelines regulating entities engaged in payment aggregation. The PA Directions apply to all bank and non-bank entities undertaking the business of a Payment Aggregator (PA), defined as an entity that facilitates the aggregation of payments made by customers to merchants through one or more payment channels (physical or virtual) for the purchase of goods, services, or investment products, and subsequently settles the collected funds to such merchants. Non-bank entities are required to seek authorisation from the RBI to operate as a PA, and must comply with stringent governance, capital adequacy, customer due diligence, escrow account maintenance, data security, and reporting obligations prescribed under the PA Directions. Banks undertaking PA business do not require separate authorisation but must comply with the applicable conduct and operational requirements.

As regards third-party access to digital information in bank accounts, India does not have a specific standalone law governing such access in the manner of open banking frameworks in other jurisdictions. However, customer confidentiality and data protection are governed by a combination of statutory provisions and regulatory directions. The RBI has periodically issued directions, guidelines, and circulars requiring regulated entities to maintain the confidentiality and privacy of customer information. For example, the Reserve Bank of India (All India Financial Institutions - Know Your Customer) Directions, 2025 (KYC Master Directions) stipulate that regulated entities shall maintain secrecy regarding customer information arising out of the contractual relationship and shall not divulge such information for purposes such as cross-selling without the express consent of the customer, except where disclosure is compelled by law, required in the public interest, necessary for the interest of the regulated entity, or made with the customer's express or implied consent. Similar secrecy and confidentiality obligations have been prescribed in the entity-specific KYC Directions issued by the RBI, for Commercial Banks, NBFCs, Local Area Banks, and other regulated entities.

Furthermore, Payment Aggregators are required under the PA Directions to undertake customer due diligence of their merchants in accordance with the KYC Master Directions and to comply with data storage, security, and reporting requirements as prescribed by the RBI.

Law stated - 8 September 2026

Online identity

- 14** | 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?

In India, the regulatory framework for Know-Your-Customer (KYC) and Anti-Money Laundering (AML) processes is primarily governed by the Prevention of Money Laundering Act, 2002 (PMLA) and its associated rules. The Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and Insurance Regulatory and Development Authority of India (IRDAI) are key regulatory bodies overseeing compliance in their respective

sectors. These regulations mandate financial institutions to implement robust measures for customer identification, due diligence, and transaction monitoring to prevent money laundering and terrorist financing activities. The PMLA, along with the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, require entities to maintain records of transactions and report suspicious activities to the Financial Intelligence Unit-India (FIU-IND).

The RBI has withdrawn its earlier consolidated Master Direction on Know Your Customer (KYC) and has, in its place, issued separate Know Your Customer directions for each category of regulated entities, including for Commercial Banks, NBFCs, Local Area Banks, and other regulated entities (collectively, the KYC Directions), each containing the KYC requirements applicable to the specific category of regulated entity. The KYC Directions regulate, inter alia, the customer identification and due diligence procedures to be followed by the RBI-regulated entities (REs) while undertaking a transaction. The KYC Directions provide, inter alia, that for the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, REs shall, at their option, rely on customer due diligence done by a third party, subject to certain conditions, including the following:

- records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry;
- adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay;
- the third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PMLA;
- the third party shall not be based in a country or jurisdiction assessed as high risk; and
- the ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

The KYC Directions now require that customer due diligence records or information be obtained from the third party immediately, removing the two-day grace period which previously applied. This change underscores the importance of timely coordination and system integration between regulated entities and the third parties engaged by them for the purpose of undertaking customer due diligence.

Law stated - 8 September 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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?

Any person in India or abroad may register country code top level domain names (CCTLDN) with a domain name registrar accredited with the '.in' registry. There is no residence or nationality requirement, and a registrant need not be an Indian citizen or a company incorporated in India. The '.in' registry is an autonomous body operating under the National Internet Exchange of India (NIXI) and is tasked with maintaining the '.in' country code, ensuring the operational stability, reliability and security of the domain.

Law stated - 8 September 2026

IP ownership

- 16** | 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?

A domain name is not itself ordinarily the subject of copyright protection in India, and protection is generally afforded through trademark law and the tort of passing off, copyright being relevant to the content of the website rather than to the address at which it is located. In view of the judicial precedents in India, the courts have construed domain names as similar to trademarks and have upheld trademark infringement and passing-off claims filed by trademark owners against users operating with the same or deceptively similar domain names.

Law stated - 8 September 2026

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

In terms of the Information Technology Act, 2000 (IT Act), it is required to be ensured that any advertisement published or transmitted through any website on the internet does not contain any obscene material, any material containing sexually explicit acts or conduct, and any material depicting children in an obscene, indecent or sexually explicit manner. In addition to the above, the Advertising Standards Council of India (ASCI) prescribes the code for self-regulation in advertising, the ASCI Code, which may be adopted by persons publishing advertisements on the internet. Adherence to the ASCI Code is voluntary in relation to online advertising and is not mandated by law. However, with respect to content on television, adherence to the ASCI Code is mandatory under the Cable Television Networks (Regulation) Act, 1995.

In the digital sphere, the ASCI guidelines have become the de facto benchmark referenced by the Ministry of Consumer Affairs when evaluating advertising complaints, major

platforms cooperate with ASCI takedown requests, and ASCI's National Advertising Monitoring Service reviews violations and escalates non-compliance to the Central Consumer Protection Authority (CCPA). The CCPA may impose penalties of up to 1 million Indian rupees on individuals and 5 million Indian rupees on entities in respect of misleading advertisements, issue cease and desist orders, and prohibit an endorser from making any endorsement for up to three years. ASCI processed 1,409 influencer violations through November 2025, of which ninety-four per cent involved failures of disclosure.

Given the surge in e-commerce platform advertising, the Consumer Protection (E-Commerce) Rules, 2020 (E-Commerce Rules) were introduced to establish duties and liabilities for various e-commerce entities and marketplace sellers. The E-Commerce Rules define an e-commerce entity as 'any person who owns, operates or manages a digital facility/ platform for electronic commerce'. In respect of advertising practices, the E-Commerce Rules mandate that sellers and inventory e-commerce entities (those owning inventory and selling directly to consumers) must: (1) ensure advertisements align with the actual characteristics, access conditions, and usage conditions of the goods/ services; and (2) accept returns/ discontinue services and provide refunds when products/ services fail to match their advertised characteristics. Marketplace e-commerce entities are required, among other obligations, to obtain undertakings from platform sellers guaranteeing that product descriptions, images, and content accurately reflect the actual appearance, nature, quality, purpose, and features of goods/services as claimed.

Additionally, there are certain laws and guidelines that prohibit the advertising and publication of certain specific types of content. A violation of these laws will entail consequences under those respective laws, including imprisonment. An illustrative list of such regulations is:

- the Bharatiya Nyaya Sanhita, 2023 (replacing the earlier Indian Penal Code, 1860) prohibits any person from selling, advertising or otherwise distributing any obscene material (such as books, pamphlets, drawings, paintings and representations). It also prohibits any person from distributing, circulating or advertising any picture or any printed or written document that is grossly indecent;
- the Cigarettes and other Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply and Distribution) Act, 2003 prohibits all direct and indirect advertising of tobacco products in all media;
- the Flag Code of India, 2002 prohibits the use of the Indian national flag in any form of advertisement;
- the Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954 prohibits the advertisement of certain drugs and of misleading advertisements;
- the Prize Chits and Money Circulation Schemes (Banning) Act, 1978 prohibits advertisements relating to prize chit and money circulation schemes;
- the Drugs and Cosmetics Act, 1940 prohibits advertisements for any drug or cosmetic from using reports of tests or analysis of the Central Drugs Laboratory or by a government analyst;
- the Cable Television Networks Rules, 1994 prohibit any advertisement promoting the production, sale or consumption of cigarettes, wine, liquor or other intoxicants through the cable service;

- the Food Safety and Standards Act, 2006 prohibits advertisement relating to the standard, quality, quantity or grade composition, and no representation concerning the need for, or the usefulness of, any food can be made that is misleading or deceiving or that contravenes the provisions of the food safety laws; and
- the Promotion and Regulation of Online Gaming Act, 2025, Section 6 of which prohibits the advertisement or promotion of online money games, directly or indirectly, across any media including digital platforms, contravention being punishable with imprisonment of up to two years, a fine of up to 5 million Indian rupees, or both.

Additionally, the Guidelines for Prevention and Regulation of Greenwashing or Misleading Environmental Claims, 2024 were issued by the Central Consumer Protection Authority to prevent deceptive environmental marketing practices. These guidelines define 'greenwashing' as deceptive or misleading practices involving concealing, omitting, or hiding relevant information through exaggerated, vague, false, or unsubstantiated environmental claims, including the use of misleading words, symbols, or imagery that emphasise positive environmental aspects while downplaying harmful attributes. The guidelines prohibit the use of generic environmental terms like 'clean', 'green', 'eco-friendly', 'carbon-neutral', 'natural', 'organic', and 'sustainable' without adequate, accurate and accessible qualifiers and substantiation. All environmental claims must be supported by accessible verifiable evidence based on independent studies or third-party certifications, and advertisers must make adequate disclosures of all material information either in the advertisement or through QR codes or URLs. Further, restrictions on the association of SEBI-regulated entities with unregistered financial influencers, introduced by SEBI's circulars dated October 22, 2024 and January 29, 2025, are addressed above in the context of financial services advertising.

Advertisers deploying generative tools must also account for the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (Amendment Rules, 2026). Promotional audio, visual or audio-visual content which is artificially or algorithmically created or altered so as to appear real, and which portrays an individual or event indistinguishably from reality, constitutes synthetically generated information. Such content must be prominently labelled and embedded with permanent metadata or other appropriate technical provenance mechanisms, to the extent technically feasible, including a unique identifier identifying the computer resource used to generate it, and platforms are expressly prohibited from enabling the modification, suppression or removal of those markers. ASCI has moved in the same direction, requiring that AI-generated influencer content be explicitly labelled and that a virtual influencer disclose upfront and prominently that consumers are not interacting with a real human being, and releasing draft guidelines in May 2026 requiring brands to disclose the use of artificial intelligence in advertising.

Law stated - 8 September 2026

Targeted advertising and online behavioural advertising

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

The term 'online advertising' has not been specifically defined under Indian law. However, laws that regulate publication or advertisement of content in physical form are medium agnostic and are equally applicable to content over the internet. Further, as per Section 2(1) of the Consumer Protection Act, 2019 (CPA 2019), 'advertisement' means any audio or visual publicity, representation, endorsement or pronouncement made by means of, inter alia, electronic media, internet or website and includes any notice, circular, label, wrapper, invoice or such other documents. Accordingly, advertisements need to comply with the CPA 2019, in addition to other laws that regulate advertising.

In December 2023, the Department of Consumer Affairs (Ministry of Consumer Affairs, Food and Public Distribution), notified the Guidelines for Prevention and Regulation of Dark Patterns, 2023 (Dark Pattern Guidelines). These Guidelines came into effect from February 01, 2024, and apply to all platforms and advertisers systematically offering goods or services in India, including those based outside India but targeting Indian consumers.

The Dark Pattern Guidelines define 'dark patterns' as any practice or deceptive design pattern using user interface or user experience interactions designed to mislead, trick, or manipulate users into making unintended actions, including unintended purchases, subscriptions, or sharing personal information. The Guidelines identify thirteen specific types of dark patterns, including false urgency, basket sneaking, confirm shaming, forced action, nagging, trick wording, drip pricing, bait and switch, disguised advertisement, and SaaS billing among others. Such practices fall within the definition of unfair trade practices in Section 2(47) of the CPA 2019, and platforms are prohibited from deploying them and must ensure transparency in their advertising and user interface design. Violations can result in penalties under the CPA 2019.

In terms of the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (CCPA Guidelines) issued by the Central Consumer Protection Authority, targeted advertising and online behavioural advertising are regulated under the broader framework of consumer protection and advertising standards. The CCPA Guidelines apply to all advertisements regardless of form, format or medium, including digital platforms and online advertising. While the CCPA Guidelines do not specifically address targeted advertising or require particular notices or consents for behavioural advertising, they establish comprehensive standards for truthful and non-misleading advertising practices that apply to all forms of digital marketing.

The CCPA Guidelines include specific provisions under Regulation 8 governing children-targeted advertisements. Advertisements that address, target, or use children are subject to stringent restrictions and must not: (1) encourage dangerous behaviour or exploit children's inexperience; (2) exaggerate product features leading to unrealistic expectations; (3) imply social consequences for not purchasing products; (4) include direct purchase exhortations to children or requests to persuade parents; (5) feature children in advertisements for prohibited products like tobacco or alcohol; (6) claim health or intelligence benefits without scientific substantiation; or (7) be published for medical services, drugs, or cosmetic surgery adverse to children's health. Additionally, junk food advertisements including chips and carbonated beverages are prohibited during children's programming or on channels exclusively for children, and promotional gifts that encourage unnecessary purchases or promote illogical consumerism are discouraged.

Further, to curb the menace of Unsolicited Commercial Communications (UCC), including spam calls, auto-diallers and robo-calls, the Telecom Regulatory Authority of India (TRAI) has, from time to time, amended the Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR, 2018). Most recently, TRAI notified the Telecom Commercial Communications Customer Preference (Second Amendment) Regulations, 2025 (2025 Telecom Regulations) on February 12, 2025, which came into force thirty days from publication (with certain provisions coming into force after sixty days).

The 2025 Telecom Regulations, inter alia: (1) revise the categorisation of commercial communications into Transactional, Service (based on Inferred Consent or Explicit Consent), Promotional, and Government messages; (2) mandate that all commercial communications originate only from designated number series allotted by DoT, with entities using undesignated number resources facing suspension or disconnection of their telecom resources; (3) require Senders to notify the Originating Access Provider in advance about the use of Auto Dialer or Robo-Calls and the intended objective of such calls; (4) prohibit call management applications from tagging, blocking, filtering, or restricting incoming calls or messages originating from designated number series assigned for commercial communications or Government communications; (5) strengthen provisions against Unregistered Telemarketers (UTMs), with stricter thresholds (five complaints from unique recipients within ten days) for initiating action; and (6) expand the definition of UCC to include any message or call made to deceive or attempt to deceive the recipient, thereby addressing fraudulent communications.

Furthermore, after the remaining provisions of the DPDP Act are brought into force, any processing of digital personal data for behavioural targeting must satisfy the notice and consent requirements of Sections 5 and 6 of the DPDP Act and Rule 3 of the DPDP Rules. Notices must be standalone, itemised, in plain language and understandable independently of any other document, must identify the categories of personal data and the specific purposes of processing, and must provide a mechanism for withdrawal of consent, exercise of rights and submission of grievances, withdrawal being as easy as the giving of consent. Verifiable parental consent will be required before processing the personal data of any person under the age of eighteen, which will require substantial re-engineering of consumer-facing advertising technology stacks.

Law stated - 8 September 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

Yes. In addition to certain industry-specific laws, the Consumer Protection Act, 2019 (CPA 2019) prohibits, inter alia, the following trade practices used for the purpose of promoting the sale, use or supply of any goods, or the practice of making any statement that:

- falsely represents that the goods or services are of a particular standard, quality, quantity, style or model;
- falsely represents any re-built, second-hand, renovated, reconditioned or old goods as new goods;

- represents that the goods or services have sponsorship, approval, performance, characteristics, uses or benefits that such goods or services do not have;
- makes a false or misleading representation concerning the need for, or the usefulness of, any goods or services;
- gives to the public any warranty or guarantee of the performance or efficacy of a product that is not based on proper tests; and
- permits the publication of any advertisement for the sale of goods or services at a bargain price that are not intended to be offered for sale at such price.

As per Section 2(28) of the CPA 2019, an advertisement that (1) falsely describes such product or service; (2) gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; (3) conveys an express or implied representation that, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or (4) deliberately conceals important information, will be construed as a misleading advertisement in relation to any product or service. Misleading advertisements are not permitted under the CPA 2019.

Further, the Central Consumer Protection Authority (CCPA), has explicit powers to investigate and penalise misleading or unfair online advertisements, including imposing fines and mandating corrective advertisements. In June 2022, the CCPA issued Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements (CCPA Guidelines) to curb false and misleading advertisements and protect consumer interest. The CCPA Guidelines prescribe specific conditions for valid, non-misleading advertisements, requiring truthful and honest representations that do not exaggerate benefits or present unsubstantiated claims as universally accepted when significant contrary views exist. The Guidelines also provide an exception for occasional and unintentional lapses in fulfilling advertised claims, provided the claim is typically achievable by the advertised product, and the advertiser takes prompt corrective action. Additionally, the CCPA Guidelines introduce new regulatory concepts including 'bait advertisements', 'free claims advertisements', and 'children targeted advertisements' to address specific advertising practices that may mislead consumers.

The Advertising Standards Council of India (ASCI) may call upon advertisers and advertising agencies to substantiate all descriptions, claims and comparisons that can be objectively ascertained. For instance, with respect to food and beverages, the ASCI Code for Self-Regulation in Advertising (ASCI Code) mandates that advertisements should not be misleading or deceptive. Specifically, advertisements should not mislead consumers to believe that consumption of the product advertised will result directly in personal changes in intelligence, physical ability or exceptional recognition. Such claims, if made in advertisements, should be supported with evidence and with adequate scientific basis. In the context of misleading advertising, the ASCI has recently issued guidelines for celebrities in advertising (Celebrity Guidelines). These Celebrity Guidelines have been developed to ensure that claims made in advertisements featuring celebrities or celebrity endorsements are not misleading, false or unsubstantiated. The Celebrity Guidelines impose certain obligations on the advertiser as well as the celebrity, for example:

- it is the duty of the advertiser to make sure that the celebrity they wish to engage in an advertisement is aware of the ASCI Code and such advertisements should not violate any guidelines of the ASCI Code;

- celebrities should not participate in advertising any products that, by law, require a health warning;
- celebrities should also not participate in advertising products, treatments or remedies that have been banned under the Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954 and Drugs and Cosmetics Act, 1940 and the rules thereunder;
- endorsements, representations of opinions or preference of celebrities in the advertisement must reflect their genuine opinion and must be based upon adequate information or experience with the product or service being advertised; and
- celebrities should do their due diligence to ensure that all descriptions, claims and comparisons made in the advertisement they appear in or endorse are capable of being objectively ascertained and capable of substantiation and should not mislead or appear deceptive.

ASCI's Guidelines for Influencer Advertising in Digital Media, most recently updated in April 2025, require every advertisement published by an influencer on the influencer's own account to carry a disclosure label clearly identifying it as an advertisement. Material connection is defined broadly and extends beyond monetary compensation to free or discounted products, including unsolicited products, gifts, contest and sweepstakes entries, trips or hotel stays, media barter, coverage, awards and any family or employment relationship. Disclosure must be upfront and prominent, must not be buried among hashtags or links, and must not appear only in a profile page or biography, at the end of a post or video, or anywhere requiring the user to click 'more'. A virtual influencer, or AI-generated content, must additionally disclose, upfront and prominently, that consumers are not interacting with a real human being.

Law stated - 8 September 2026

Restrictions

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

Yes. Advertising of products such as cigarettes, tobacco and its derivatives, alcohol, infant milk substitutes, certain drugs, firearms, gambling and lotteries are prohibited under different laws, whether on the internet or otherwise. These restrictions and prohibitions are medium agnostic and would be applicable to both digital as well as other forms of advertisement.

India's regulatory approach to online gaming has evolved significantly, with both central and state authorities adopting measures to address concerns relating to online money gaming, consumer protection and advertising practices. The legal position remains subject to ongoing constitutional and federalism-related questions, particularly concerning the allocation of legislative competence between the Union and States in relation to gaming and gambling. Advertisers and digital platforms should therefore monitor developments closely and ensure compliance with applicable restrictions and sector-specific guidance.

The CCPA has also issued advisories directed at preventing celebrities and influencers from endorsing betting platforms.

Separately, the Amendment Rules, 2026 prohibit specified categories of synthetically generated content outright, including child sexual exploitation material, non-consensual intimate imagery, obscene or sexually explicit content, false documents or electronic records, and synthetic depictions of explosives or arms.

Law stated - 8 September 2026

Direct email marketing

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

Prior to the Digital Personal Data Protection Act, 2023 (DPDP Act), there were no specific regulations in India governing marketing activities undertaken through email or other similar distance marketing methods, apart from sector-specific guidelines. However, with the commencement of the DPDP Act and the Digital Personal Data Protection Rules, 2025 (DPDP Rules), any processing of personal data for direct marketing purposes now falls under its purview. A data fiduciary must ensure compliance with the notice and consent requirements specified in Sections 5 and 6 of the DPDP Act and Rule 3 of the DPDP Rules, which take effect on 13 May 2027, being eighteen months from the publication of the DPDP Rules in the Official Gazette on November 13, 2025 under the phased commencement schedule notified by the Central Government. Rule 3 requires the notice to be clear, in plain language and understandable independently of any other document, to describe the categories of personal data and the specific purposes of processing, and to disclose the mechanisms for withdrawal of consent, exercise of rights and submission of grievances, withdrawal being as easy as the giving of consent. The consent given by the data principal must be free, specific, informed, unconditional, and unambiguous with a clear affirmative action. Rule 4, which governs the registration and obligations of consent managers, takes effect earlier, on 13 November 2026.

Additionally, in relation to SMS, the Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCPR) prohibit the sending of unsolicited commercial communications (UCC) in India. UCC is defined under the TCCPR to mean any commercial communication (which includes a call or SMS for promoting products or services) that is not as per the consent or the registered preferences of the recipient of the call or SMS. The responsibility to ensure compliance with the TCCPR is imposed on the telecom service provider. Any person required to share commercial communications is required to obtain services of the telecom services provider and comply with codes of practice (CoP) published by such telecom service provider. These CoP prescribe processes for, inter alia, registering consent of the customer and whitelisting templates for transactional and promotional messages.

TRAI's regulation-making powers in this area operate within a statutory framework which is itself in transition, the Telecommunications Act, 2023 having repealed the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933 and being brought into force in stages.

Law stated - 8 September 2026

ONLINE PUBLISHING

Hosting liability

- 22** | 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?

Under the Information Technology Act, 2000 (IT Act) an intermediary (ie, in relation to an electronic record, any person who on behalf of another receives, stores, transmits or provides any service with respect to that record, and expressly includes online marketplaces and similar platform providers) is granted a “safe harbour” protection in respect of third-party content hosted on their platforms. Section 79 of the IT Act provides that an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by it, subject to the intermediary complying with the conditions prescribed under the provision and exercising due diligence while discharging its functions. However, this exemption is conditional upon the intermediary observing the due diligence obligations specified under the IT Rules, 2021, which apply to entities that qualify as intermediaries.

Accordingly, for an intermediary to be exempt from liability under the IT Act for third-party information, data or communication links, and receive protection under Section 79 minimising the liability of the intermediary, it must satisfy certain conditions, including:

- the intermediary's role must be limited to providing access to information made available by third parties;
- the intermediary must not initiate the transmission of data made available by third parties;
- the intermediary must not select the receiver of the transmission; and
- the intermediary must not select or modify the information contained in the transmission, or have any control over such information.

It also needs to be demonstrated that the intermediary has observed ‘due diligence’ in discharging its duties under the IT Act and the IT Rules, which require that the intermediary should not conspire, abet, aid or induce the commission of the unlawful act and should also expeditiously remove or disable access to objectionable content upon receiving knowledge and comply with other takedown and grievance redressal obligations under the IT Rules.

Law stated - 8 September 2026

Content liability

- 23** | 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?

Under the Information Technology Act, 2000 (IT Act) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines), an intermediary is required to observe due diligence in discharging its duties. Rule 3(1)(a), as substituted, requires an intermediary to publish prominently on its website, mobile based application or both, its rules and regulations, privacy policy and user agreement, in English or in any language specified in the Eighth Schedule to the Constitution, so that a person may access or use its computer resource in the language of his choice, and to ensure compliance with the same.

As per the IT Act, where the website provider is an intermediary, it may be entitled to avail of safe harbour provisions, provided it meets the requirements under the IT Act and Intermediary Guidelines. However, where the website provider itself uploads content on the website, it may be held liable if such content is not in accordance with the provisions of the IT Act, the relevant rules and the guidelines.

Further, as per the code of ethics provided under the Intermediary Guidelines, a publisher shall take into consideration the following factors, when deciding to feature or transmit or publish or exhibit any content, after duly considering the implications of any content as falling under the following categories, and shall exercise due caution and discretion in relation to the same, namely: (1) content that affects the sovereignty and integrity of India; (2) content that threatens, endangers or jeopardises the security of the state; (3) content that is detrimental to India's friendly relations with foreign countries; and (4) content that is likely to incite violence or disturb the maintenance of public order.

Law stated - 8 September 2026

Shutdown and takedown

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

The position has evolved significantly and is presently the subject of appellate litigation. Historically, if an Internet Service Provider (ISP) had knowledge, either by itself or through being informed by an affected person, that content stored, hosted or published on a web page contained unlawful material, including defamatory content, it was under an obligation to disable, remove access to or take down such information expeditiously. Following the judgement of the Supreme Court of India in *Shreya Singhal v Union of India*, online information may be blocked only under Section 69A of the IT Act or pursuant to an order of a court of competent jurisdiction, Section 79 being a safe harbour provision rather than a source of blocking power.

Law stated - 8 September 2026

INTELLECTUAL PROPERTY

Data and databases

|

25 | Are data and databases protected by IP rights?

If a database on a website constitutes a copyrightable work in terms of the Copyright Act, 1957 and the website provider is the owner of such copyrightable work, the provider can prevent or restrict other people from using or reproducing data from the database. Section 14 of the Copyright Act confers upon the owner exclusive rights including the right of reproduction, which includes storage, together with rights of translation, adaptation, communication to the public and issuing copies of the work to the public, and doing any of these acts without a licence amounts to infringement under Section 51 unless the act falls within one of the exceptions in Section 52. There is at present no specific exception under Indian copyright law for text and data mining, nor any exception designed to exempt the training of artificial intelligence systems from potential infringement.

Law stated - 8 September 2026

Third-party links and content

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

Any hyperlinking of a domain name of a third-party website without the express permission of the third-party trademark owner may be construed as infringement under the trademark law and copyright law.

Law stated - 8 September 2026

27 | 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?

No. Storage or use of any third-party content on the website without the consent of the third-party content provider may constitute copyright infringement, unless such use is recognised as fair use under the Copyright Act, 1957 (Copyright Act). In terms of the Copyright Act, the potential consequences for copyright infringement could be civil as well as criminal in nature. For instance, in the case of copyright infringement, the owner of the copyright may be entitled to civil remedies such as an injunction and compensation or direct damages; or there may be criminal remedies in the form of imprisonment or fines in cases where a person knowingly infringes or abets the infringement of copyright.

Law stated - 8 September 2026

Metaverse and online platforms

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

Due to the complex nature of operations in the metaverse, it may be difficult to identify the infringers and the infringements. Artificial intelligence and automated systems may be deployed for ensuring that infringement of copyright, trademark or patent in the metaverse is identified and addressed.

Further, there is no dedicated law dealing with infringement of copyright, trademark or patent in the metaverse, and therefore the intellectual property protection laws that are currently adopted in the physical, or real, world may also apply to the metaverse.

Operators of immersive environments should also note that synthetic depictions of individuals within such environments may engage the obligations under the Amendment Rules, 2026. Avatars, digital doubles and other audio, visual or audio-visual representations generated or altered within a metaverse or similar immersive environment may fall within the definition of synthetically generated information under Rule 2(1)(wa) where they are created or modified using a computer resource in a manner that renders them, or is likely to render them, indistinguishable from a real person or a real-world event, for instance where a user's avatar is generated from, or animated using, a real individual's likeness, voice or biometric data so as to appear authentic.

Where an operator offers a computer resource enabling users to create, generate, modify or alter such synthetic depictions, it may be treated as an intermediary offering synthetic content generation tools for the purposes of Rule 3(3) of the IT Rules, 2021, and may accordingly be required to deploy reasonable and appropriate technical measures, including automated tools, to prevent the generation or sharing of synthetic content that violates any law, such as non-consensual intimate imagery, deceptive portrayals of real individuals or events, and false depictions used to facilitate fraud or impersonation within the immersive environment.

Synthetic depictions that are otherwise permitted must be prominently labelled and embedded with permanent metadata or other appropriate technical provenance mechanisms, to the extent technically feasible, including a unique identifier for the computer resource used to generate them, and the operator must not enable the modification, suppression or removal of such labels, metadata or identifiers. Operators should also factor in the enhanced periodic disclosure obligations applicable to platforms offering synthetic content generation tools, and the fact that non-compliance with these obligations may be treated as a failure of due diligence capable of jeopardising the safe harbour otherwise available under Section 79 of the IT Act.

Law stated - 8 September 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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 – trademarks

Section 30(3) of the Trade Marks Act, 1999 (Trade Marks Act) recognises exhaustion of rights of the proprietor of a trademark after the first sale of goods. It provides that once goods bearing a registered trademark are lawfully acquired by a person, any subsequent sale or commercial dealing in those goods, either by that person or by someone deriving rights through them, will not amount to trademark infringement merely because:

- the trademark was later assigned to a different owner after the goods were acquired; or
- the goods were placed on the market by the trademark owner or with their consent.

Further, the Trade Marks Act provides that the aforesaid provision does not apply where the owner has legitimate reasons to oppose dealings in the goods, particularly if the goods are changed or impaired after they have been made available in the market.

Exhaustion of rights – copyrights

Copyright covers a wide variety of works in its contours. These include artistic, dramatic, literary, cinematic and academic works. The owner of a copyright has a bundle of rights in respect of the work. This bundle of rights can be traced under Section 14(1) of the Indian Copyright Act, 1957, which makes it clear that irrespective of the kind of work in question, it is the exclusive right of the owner to issue copies of the work to the public or communicate it to the public. The Doctrine of First Sale in relation to copyright is work-specific and is not uniform and varies in its application due to the classification of works into different kinds. This means that once the copyright holder sells someone some work, such person may be free to sell it further. However, it may not be permissible to make copies of such work and sell it further.

Exhaustion of rights – patents

India recognises the principle of international exhaustion under Section 107-A(b) of the Indian Patents Act, 1970, which provides that *'importation of patented products by any person from a person who is duly authorised under the law to produce and sell or distribute the product, shall not be considered as an infringement of patent rights'*.

Essentially, the exclusive rights of the patent owner are lost when there is a sale of such patent. Accordingly, the person purchasing a patent can use or resell that product without infringing the patent.

There is no specific law dealing with exhaustion of rights or the first sale doctrine in relation to the metaverse.

Law stated - 8 September 2026

Administrative enforcement

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

Yes. For instance, the Copyright Act, 1957 empowers police authorities in India to seize infringing copies if the officer concerned is satisfied that an offence in respect of the infringement of copyright in any work has been committed. There have also been a few occasions where courts have passed orders in the nature of Mareva injunctions, or what is commonly known as a freezing order in India, to restrain the defendants from disposal of their assets until conclusion of the trial or pending judgment in infringement actions instituted by intellectual property owners.

Law stated - 8 September 2026

Civil remedies

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

Ordinarily the relief sought by intellectual property (IP) owners include:

- permanent injunction restraining defendants from infringing the owner's IP rights;
- permanent injunction restraining the defendant from selling the infringing product;
- destruction of goods infringing the IP rights;
- submission or seizure of books of accounts of the defendant;
- compensation in the nature of damages; and
- in a few cases, punitive damages.

Indian courts do not ordinarily grant punitive damages, but there have been a few instances where they have been awarded in matters involving IP infringement.

Further, authorities under IP laws in India can also issue search orders and freezing injunctions. For instance, the Copyright Act, 1957 empowers police authorities in India to seize infringing copies if the officer concerned is satisfied that an offence in respect of the infringement of copyright in any work has been committed. There have also been a few occasions where courts have passed orders in the nature of Mareva injunctions, or what is commonly known as a freezing order in India, to restrain the defendants from disposal of their assets until conclusion of the trial or pending judgment in infringement actions instituted by IP owners.

Law stated - 8 September 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

32 | 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?

While 'personal data' has not been defined under the Information Technology Act, 2000 (IT Act), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) framed thereunder define personal information as any information that relates to a natural person and that, directly or indirectly, is capable of identifying such person. Further, the SPDI Rules define 'sensitive personal data or information' as such personal information that consists of information relating to:

- passwords;
- financial information, such as bank accounts, credit cards, debit cards or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information; and
- any details relating to the above as provided to body corporates for providing services.

Any information that is freely available in the public domain or may be furnished as under the Right to Information Act, 2005 or any other law will not be considered as sensitive personal data or information.

In relation to collection of information, the SPDI Rules prescribe that any body corporate that collects, receives, stores, deals or handles personal information is required to frame a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view to persons providing such information under lawful contract. Such privacy policy must be published on the body corporate's website and shall include information pertaining to:

- statement of practice and policies;
- type of sensitive information being collected;
- purpose and usage of such information;
- circumstances in which such sensitive personal information may be disclosed; and
- security practices and procedures for securing against unauthorised access or disclosure of such information in accordance with the SPDI Rules.

In addition to the above, any body corporate collecting 'sensitive personal data or information' must obtain written consent from the provider of information (i.e., the data subject) regarding the purpose of usage of such information as per the SPDI Rules. Accordingly, while collecting such information, the body corporate is required to ensure that the data subject is made aware that the information is being collected, the purpose for which the information is being collected, the intended recipients, and the name and address of the agency responsible for collecting and retaining such information.

The SPDI Rules further stipulate that sensitive personal data can be collected only for a lawful purpose connected with the function of the body corporate, and only when the

collection of such data is considered necessary for such purpose. Once such a purpose is fulfilled, the body corporate can no longer retain such information.

Prior to the collection of such data, the body corporate is required to provide an option to the data subjects not to provide the information sought to be collected. If the data subject does not provide consent or subsequently withdraws his or her consent, the body corporate has the option not to provide any services or goods for which the said information was sought.

The SPDI Rules also prescribe that the data subject must be given an opportunity to review the information provided and ensure that any inaccuracy or deficiency in the information provided is corrected. While no specific mechanism has been prescribed, such opportunity should be available to data subjects as and when requested by them.

In case of any discrepancies or grievances of the data subjects, the body corporates collecting the data must address the same in a time bound manner. For this purpose, the body corporate has to designate a grievance officer and publish his name and contact details on its website. The grievance officer is required to resolve any such grievance within one month from the date of receipt of grievance.

The SPDI Rules also impose obligation on the body corporates collecting personal data to implement reasonable security practises. Accordingly, as a part of the SPDI Rules, the Central Government has prescribed the 'ISO/IEC 27001 standard for Information technology – Security techniques – Information security management system – Requirements', issued by the International Organization for Standardization and International Electrotechnical Commission (ISO 27001), as one of the standards that a body corporate dealing with sensitive personal information may implement.

Separately, India is in the process of overhauling its data protection regime with implementation of the Digital Personal Data Protection Act, 2023 (DPDP Act), which has been enacted and is being operationalised through a staggered implementation framework. While certain institutional and procedural provisions of the DPDP Act have come into force and the Digital Personal Data Protection Rules, 2025 have already come into force, the substantive obligations relating to notice and consent, data principal rights, processing of children's data, cross-border transfers and enforcement are scheduled to be implemented in phases, with full operationalisation expected by May 2027. Once fully in force, the DPDP Act read with the Rules will introduce a comprehensive and uniform framework governing the processing of personal data by all data fiduciaries, including foreign entities processing personal data of individuals located in India, and will require compliance with principles such as lawful processing, purpose limitation, data minimisation, consent standards and accountability.

It defines personal data as any data about an individual who is identifiable by or in relation to such data. Entities collecting personal data will have to undertake the prescribed compliances under the DPDP Act including obtaining free, specific and informed consent prior to collection of personal data, specifying purpose of processing of data, ensuring implementation of data minimisation requirements, and upholding other rights of data principals like right to access, correction, erasure of data, etc.

Law stated - 8 September 2026

Registration and appointment of data protection officer

- 33** | 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. There is no requirement for parties involved in the processing of personal data to register with any regulator or appoint an in-house data protection officer under Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

There is however a requirement for body corporates collecting personal data to appoint a grievance officer to address the discrepancies and grievances of the providers of such information in a timely manner. The name and contact details of the grievance officer must be uploaded on the website of the body corporate collecting personal data.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act) read with the Digital Personal Data Protection Rules, 2025, which are being implemented in a phased manner, do not prescribe any general requirement for registration with a regulator for processing personal data. The DPDP Act requires all data fiduciaries to put in place an effective grievance redressal mechanism and designate a point of contact for data principals. The obligation to appoint a data protection officer applies only to 'significant data fiduciaries', as may be notified by the Central Government, and such officer is required to be based in India.

Law stated - 8 September 2026

Extraterritorial issues

- 34** | 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 Information Technology Act, 2000 (IT Act) has extraterritorial jurisdiction to the extent that it is applicable to any contravention committed outside India by any person, irrespective of his or her nationality, if such act or conduct constituting the offence committed outside India involves a computer or a computer system or a computer network located in India. In other words, applicability of the IT Act is agnostic to the physical presence of servers in India, and to the extent that users in India can access services by using a computer, computer system or computer network in India, the provisions of the IT Act would be applicable.

With respect to the transfer of sensitive personal information, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 framed under the IT Act allow a body corporate to transfer such data to any other body corporate or a person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, such transfer may be allowed only if it is necessary for the performance of a

lawful contract between the body corporate and the data subject or where such person has consented to the data transfer. In other words, sensitive personal data can only be transferred to another person with the consent of the data subject.

There is however a requirement for body corporates collecting personal data to appoint a grievance officer to address the discrepancies and grievances of the providers of such information in a timely manner. The name and contact details of the grievance officer must be uploaded on the website of the body corporate collecting personal data.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act), which is being implemented in a phased manner, regulates the processing of personal data of individuals by the government, companies incorporated in India and foreign entities, where such processing is in connection with any business carried on in India, any systematic activity of offering goods or services to data principals within India, or involves profiling of data principals within India. The DPDP Act restricts the transfer of personal data by data fiduciaries to such countries or territories outside India as may be notified. Further, the Digital Personal Data Protection Rules, 2025 also require data fiduciaries to meet such requirements as the central government may, by general or special order, specify in respect of making such personal data available to any foreign state, or to any person or entity under the control of or any agency of such a state.

Law stated - 8 September 2026

Bases for processing

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

According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), personal data can be collected/processed by a body corporate for any lawful purpose connected with a function or activity of the body corporate collecting such this information, and if collection of the data is considered necessary for that purpose.

The SPDI Rules permit transfer of this information to another body corporate (in India or otherwise) that maintains the same level of data protection as required under the Information Technology Act, 2000 read with the SPDI Rules, and such transfer may only be done only if this is necessary for the performance of a contract between the transferor and the data principal, or with the consent of the provider of the information.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act), which is being implemented in a phased manner, permits processing of personal data only for lawful purposes based on the consent of the data principal or for certain legitimate uses expressly recognised under the DPDP Act, including compliance with legal obligations. The DPDP Act applies extraterritorially where processing by data fiduciaries or processors outside India is in connection with business carried on in India, systematic offering of goods or services to individuals in India, or profiling of individuals in India. Cross-border transfer of personal data is permitted unless restricted by the Central Government by notification and is subject to conditions that may be specified by the Central Government.

In addition, the Digital Personal Data Protection Rules, 2025 require that notices seeking consent be clear, standalone, and written in plain language, specifying the categories of personal data processed, the purpose of processing, and the manner in which data principals may withdraw consent or exercise their rights.

Law stated - 8 September 2026

Data export and data sovereignty

- 36** | 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?

Section 75 of the Information Technology Act, 2000 (IT Act) provides for extra-territorial applicability of the IT Act, and states that the IT Act will apply to any offence or contravention committed by a person outside India, regardless of their nationality, if it involves a computer or a computer system or a computer network located in India. In other words, applicability of the IT Act is agnostic to the physical presence of servers in India, and to the extent that users in India can access services by using a computer, computer system or computer network in India, the provisions of the IT Act would be applicable.

With respect to the transfer of sensitive personal information, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) allow a body corporate to transfer such data to any other body corporate or a person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, such transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject, or where the data subject has consented to the data transfer.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act), which is being implemented in a phased manner, permits cross-border transfer of personal data unless restricted by the Central Government through notification. The DPDP Act has extraterritorial jurisdiction for processing of personal data by data fiduciaries or processors outside India where such processing is in connection with business carried on in India, systematic offering of goods or services to individuals in India, or profiling of individuals in India. In addition, the Digital Personal Data Protection Rules, 2025 empower the Central Government to prescribe requirements for disclosure or transfer of personal data to foreign States or entities under their control, and enable the imposition of data localisation or transfer restrictions for specified categories of data or classes of data fiduciaries, including on grounds of national security or public interest.

Law stated - 8 September 2026

Sale of data to third parties

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

While the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) do not expressly contemplate sale of personal data, transfer of personal information is permitted subject to fulfilment of the following conditions:

- the body corporate to whom such information is being transferred ensures the same level of data protection;
- such transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf, or provider of information has consented to data transfer in accordance with the SPDI Rules.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act) which is being implemented in a phased manner does not explicitly prohibit sale of data. However, given that consent is likely to be the primary basis for processing personal data, it is recommended to ensure, through contractual arrangements, that appropriate consent has been obtained from the data principal by the transferor to share such personal data, as well as for the receiving/transferee entity to process such personal data. In this context, the Digital Personal Data Protection Rules, 2025 require that such consent be obtained pursuant to a clear and standalone notice, specifying the nature of personal data processed, the purpose of processing, and enabling the data principal to withdraw consent or exercise statutory rights.

Law stated - 8 September 2026

Consumer redress

38 | 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?

A person aggrieved of impermissible processing of sensitive personal data is entitled to claim damages by way of compensation under the Information Technology Act, 2000 (IT Act). Any person (including a foreign national) may claim such damages by way of compensation under the IT Act.

Further, a body corporate shall also address any discrepancies and grievances of the provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate must designate a grievance officer and publish his name and contact details on its website. The grievance officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act) which is being implemented in a phased manner, requires entities collecting personal data to undertake the prescribed compliances including obtaining free, specific and informed consent prior to collection of personal data, specifying purpose of processing of data, ensuring implementation of data minimisation requirements, and upholding other rights of data principals like right to access, correction, erasure of data, and ability to withdraw consent

for processing of data, among others. The Digital Personal Data Protection Rules, 2025 further require data fiduciaries to establish accessible and clearly disclosed mechanisms for exercising such rights, prescribe outer timelines for grievance redressal, and mandate that notices and communications enabling these rights be clear, standalone and easily understandable.

The applicability of the DPDP Act extends to the processing of personal data by data fiduciaries or data processors outside India, if such processing is either in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within India, or in connection with any activity which involves profiling of data principals in India. The Central Government however, may, by notification, restrict the transfer of personal data by a data fiduciary for processing to such country or territory outside India as may be so notified.

Law stated - 8 September 2026

Non-personal data

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

At present, India does not regulate the use of non-personal data. Separately, India is in the process of overhauling its data protection regime with the introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) which is being implemented in a phased manner, and is expected to fully be in force by May 2027. Even the DPDP Act does not regulate non-personal data.

However, in July 2020, Committee of Experts on Non-Personal Data Governance Framework (Committee) formulated by the Ministry of Electronics and Information Technology (MeitY), proposed a framework for regulating non-personal data to enable data sharing and address potential harms.

The Committee has defined three categories of non-personal data: (1) public non-personal data; (2) community non-personal data; and (3) private non-personal data. The Committee has also defined a new concept of 'sensitivity of non-personal data', as even non-personal data could be sensitive in that (1) it may relate to national security or strategic interests, (2) it may be business sensitive or confidential information, or (3) it may be anonymous data that bears a risk of re-identification.

The Committee observed that non-personal data should be regulated.

Subsequently, in May 2022, MeitY released its draft National Data Governance Framework Policy (Policy) which provides guidance on the procedures and security standards to be implemented by the government for all non-personal data handled and collected by it. The policy aims to standardise and improve the government's data collection and management. However, the same continues to be in draft stage till date.

Law stated - 8 September 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

- 40** | 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?

Certain laws such as the Companies Act, 2013 may require books of account to be maintained at the registered office of the company or such other place in India as decided by the Board and notified to the Registrar of Companies. However, according to the Information Technology Act, 2000, in the event any law requires a document, any information or other matter to be maintained in printed or written form, such requirement is considered to be satisfied even if such information or matter is made or rendered available in electronic format.

Law stated - 8 September 2026

Retention

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

Sector-specific regulations prescribe storage requirements for certain kinds of documents and records. Below is an indicative list of these sectoral regulations:

- The Information Technology Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), provides that sensitive personal data or information (SPDI) can only be retained until such time the purpose for which such SPDI was collected is achieved, or unless otherwise required by applicable law;
- The Companies Act, 2013 prescribes that any books of accounts and related vouchers, documents, etc should be retained for a period of not less than eight financial years;
- The Insurance Regulatory and Development Authority of India has issued the Insurance Cyber Guidelines, which require all registered insurance companies to maintain security logs of different systems and devices, to be retained for a minimum period of six months; and
- In accordance with the Securities Exchange Board of India Guidelines (Cyber Security & Cyber Resilience Framework for Stock Brokers/Depository Participants), stockbrokers and depository participants are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period of not less than two years.

Law stated - 8 September 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

Pursuant to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, any body corporate that possesses, deals with, or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements).

Sector-specific cybersecurity measures have also been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the Reserve Bank of India (RBI) requires banks to undertake certain security measures including, inter alia, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security.

Law stated - 8 September 2026

Data breach notification

- 43** | 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?

The Indian Computer Emergency Response Team (CERT-In), established under the Information Technology Act, 2000, is the national nodal agency which deals with cyber security incidents and responding to such incidents. It is tasked with performing certain functions including collection, analysis and dissemination of information on cyber incidents, handling cyber security incidents, issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, response and reporting of cyber incidents. Exercising such powers, CERT-In had issued the directions dated 28 April 2022 (Directions) for strengthening cyber security in India. Clarifications to the Directions were issued by CERT-In by way of frequently asked questions on 18 May 2022.

As per the Directions, all service providers, intermediaries, data centres, body corporates, and government organisations are required to report specified cyber incidents to CERT-In within six hours of detecting them or being notified of their occurrence. The scope of

reportable cyber incidents under these Directions specifically includes data breaches and data leaks.

In addition to reporting requirements under the Directions, an intermediary is required to also, not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents according to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

There are also sector-specific regulators with their own reporting requirements. For instance, the Reserve Bank of India (RBI) requires banks to comply with the cybersecurity framework for Banks, which, inter alia, requires banks to report cybersecurity incidents to the RBI within six hours.

Separately, the Digital Personal Data Protection Act, 2023 (DPDP Act), read with the Digital Personal Data Protection Rules, 2025 (DPDP Rules) both of which are being implemented in a phased manner (complete implementation expected by May 2027), introduce a dedicated personal data breach notification regime. Upon becoming aware of a personal data breach, a data fiduciary is required to notify the Data Protection Board of India without delay by way of a preliminary intimation, followed by a detailed intimation within 72 hours (or such extended period as may be permitted). The DPDP Rules further require the data fiduciary to notify affected data principals without undue delay, in a clear and concise manner, through the data principal's user account or other registered communication channels, setting out the nature of the breach, its likely consequences and remedial measures.

Law stated - 8 September 2026

Government interception

44 | 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?

In the case of *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under Article 21 of the Constitution of India, and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence.

In any case, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules) require body corporates to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the Information Technology Act, 2000 (IT Act) for

the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes. Any person or officer authorised by the government (central or state) can, inter alia, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data for cybersecurity incidents if they relate to contravention or investigation of any crime.

Similar to the SPDI Rules, the Digital Personal Data Protection Act, 2023 (DPDP Act) which is being implemented in a phased manner (with full implementation expected by May 2027), stipulate that data may be processed if it is basis a legitimate use. Legitimate uses under the DPDP Act also include fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities.

In addition to the above, Section 20 of the Telecommunications Act, 2023 (Telecom Act), in cases of public emergency, permits the Central Government, the State Government, or any officer on its behalf to:

- take temporary possession of any telecommunication service or telecommunication network from an authorised entity;
- provide for appropriate mechanism to ensure that messages of a user or group of users authorised for response and recovery during public emergency are routed on priority;
- in the interest of sovereignty and integrity of India, or preventing incitement of an offence, and for reasons to be recorded in writing order interception, detention, disclosure, blocking of specific messages or classes of communications, or suspend telecom services for specified persons, equipment, or subjects, on authorised grounds and subject to safeguards.

These safeguards have been prescribed under the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 (Telecom Rules) which include ensuring any interception only by designated senior authorities with written reasons (Union Home Secretary for the Central Government or the Secretary to the State Government in-charge of the Home Department for State Governments) Further, procedural oversight, such as time-bound validity (with caps on duration), mandatory review by a high-level review committee, and requirement to destroy intercepted messages every six months has been provided.

Law stated - 8 September 2026

GAMING

Legality and regulation

45 |

| 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?

The legal position in India has undergone a fundamental shift with the coming into force of the Promotion and Regulation of Online Gaming Act, 2025 (Gaming Act) and the Promotion and Regulation of Online Gaming Rules, 2026 (Gaming Rules) with effect from May 1, 2026.

At the outset, it is not permissible to operate an online betting or “online money gaming” business in India. The Gaming Act introduces a blanket prohibition on online money games, which would include games involving betting, wagering, or staking money with an expectation of monetary gain. The determination of whether a game qualifies as an “online money game” is undertaken by the Online Gaming Authority of India (Authority) based on factors such as (1) involvement of stakes or deposits, (2) expectation of winnings, (3) the nature of fee structures, (4) the revenue model, and (5) the monetisation or transferability of rewards. Once a game is determined to be an online money game, banks and payment intermediaries are mandatorily required to suspend or discontinue financial transactions relating to such games, effectively rendering their operation impermissible.

However, online social games (without staking or monetary rewards) and e-sports are permitted, subject to compliance with the Gaming Act and Gaming Rules. The regulatory framework for such permitted games operates as follows:

Regulatory approvals / registration

Registration is not mandatory for all online social games, unless specifically required by the Central Government based on factors such as user risk, scale, or transaction value. However, registration is mandatory for e-sports, which must be recognised and registered with the Authority. Where a game is registered or determined by the Authority, such status must be prominently disclosed on the platform.

User verification and safety requirements

The Gaming Rules introduce a new defined term, “user safety features” which encompass technical, procedural, operational, behavioural, and system-related safeguards, including age verification or age-gating mechanisms, time restrictions, parental controls, user reporting and grievance redressal mechanisms, counselling support, and fair-play and integrity monitoring tools. The application to be submitted by an online gaming service provider for determination or registration of their online games must include details related to these “user safety features”.

Payment and financial verification controls

For permitted games (ie, online social games and e-sports):

- Payment facilitators (including banks and intermediaries) must comply with directions issued by the Authority;
- Prior to processing payments, such entities may be required to verify the registration status of the game in the manner prescribed by the Authority;

- Any changes to payment mechanisms by the operator must be notified to the Authority.

Grievance redressal

A two-tier grievance mechanism is mandated, requiring users to first approach the operator, and thereafter the Authority within prescribed timelines.

Data localisation obligations

Operators are required to store specified categories of data (such as traffic data and metadata) on servers located in India, in accordance with directions issued under the Gaming Act.

In summary, while India permits operation of certain categories of online games (i.e., non-monetised social games and regulated e-sports), online betting or wagering-based gaming models are expressly prohibited. Permissible operators are subject to a compliance-heavy framework involving potential registration, user verification safeguards (including age-gating), payment verification protocols, and ongoing regulatory oversight by the Authority.

Law stated - 8 September 2026

Cross-border gaming

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

As per the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 issued under the Consumer Protection Act, 2019, no advertisement is permitted in respect of goods or services that are prohibited from being produced, sold, or provided, or whose advertisement is otherwise prohibited under applicable law.

In this context, the legal position in India has materially evolved with the coming into force of the Promotion and Regulation of Online Gaming Act, 2025 (Gaming Act) and the Promotion and Regulation of Online Gaming Rules, 2026 with effect from 1 May 2026. Under this regime, online money games, including betting, wagering, or staking-based gaming models, are subject to a blanket prohibition. Consequently, once an online game is determined to qualify as an online money game, its operation is impermissible and financial intermediaries are required to suspend or discontinue payment facilitation in relation to such games.

Accordingly, advertising of such prohibited online betting or online money gaming services would not be permissible in India, even where such services are operated from another jurisdiction or within a metaverse environment. This position flows from the principle that services which cannot be lawfully offered in India cannot be indirectly promoted to users in India.

Similarly, facilitating or providing access from India to such prohibited online money gaming services, including offshore platforms or metaverse-based offerings, would carry significant regulatory risk. The framework under the Gaming Act focuses on the availability of such games to users in India, and the prohibition is not avoided merely on account of the operator being located outside India or the use of emerging digital environments.

However, advertising and access to permitted categories of games, such as online social games without staking or monetary rewards and duly recognised e sports, would be permissible, subject to compliance with the applicable regulatory framework and advertising standards.

In summary, advertising or enabling access to online betting or wagering platforms, irrespective of whether they are hosted offshore or within a metaverse, would not be permissible under Indian law as it would amount to promoting or facilitating a prohibited activity.

Law stated - 8 September 2026

OUTSOURCING

Key legal issues

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

Outsourcing of a contract would ordinarily result in an end product, the ownership of which will be at the heart of the contractual arrangement. This will necessarily involve issues with respect to ownership of intellectual property, particularly copyright. Since copyright created in the course of a contract for service is commissioned and owned by the contractor to begin with, the outsourcing contract should contain unambiguous provisions regarding the ownership and assignment of copyright. Provisions with respect to indemnity and limitation on liability are generally highly negotiated. In a cross-border scenario, the non-resident party has to bear in mind that prior Reserve Bank of India approval may be required before any amount can be remitted on account of damages. There is substantial emphasis on meeting service-level agreements and failure may have significant business continuity issues. Dispute resolution provisions, particularly regarding the ability to obtain interim relief, may also be equally important from the perspective of the service recipient. When outsourcing services outside India, it's crucial to clearly define which country's laws govern the contract and where disputes will be resolved. Enforcement can be challenging if the provider is in another country, especially if court judgments or arbitral awards are not easily recognised across borders.

Receipt of consideration for provision of services by a service provider may be subject to taxation in India, including good and services tax (GST), depending on factors such as the specific nature or character of such services, presence of permanent establishment, availability of treaty benefits and the like. In the event such consideration is taxable in India, the service provider may be required to undertake compliances such as obtaining relevant GST and income tax registration, discharge of the applicable taxes, issuance of relevant documents such as invoices and filing of relevant tax returns in India. Additionally,

the service recipient may also be required to withhold applicable taxes and undertake requisite compliances. Accordingly, this would require a detailed examination based on specific facts.

In this regard, it may further be noted that typically, the compliances related to GST including obtaining GST registration, depositing the applicable GST on a taxable supply of service, issuance of invoice and filing of returns is on the supplier or provider of such service. However, for certain specified services, including on import of services, such compliances are required to be undertaken by the recipient of such service under the reverse charge mechanism.

Outsourcing services may also give rise to employment-related risks, particularly the risk of deemed employment or absorption. If the entity to whom the services are outsourced exercises direct control or supervision over the service provider's employees such as issuing instructions or integrating them into its own workforce, courts may treat them as its own employees, potentially requiring the entity to provide the same statutory benefits and protections as it does to its own employees.

Additionally, outsourcing services to a provider may involve sharing/ transfer of personal data with such service provider and risks in relation to ensuring that the service provider is complying with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 will entail.

Law stated - 8 September 2026

Sector-specific issues

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

Based on the nature of business, certain regulators have issued specific outsourcing guidelines and regulations in relation to the regulated entities, including:

- Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Non-Banking Financial Company – issued by the Reserve Bank of India (RBI) where banks may outsource financial services however should not outsource core management functions including internal audit, compliance function and decision-making functions like determining compliance with Know Your Customer norms for opening deposit accounts, according sanction for loans;
- Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators – issued by the RBI which regulated certain outsourcing activities by non-bank payment system operators;
- IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 – issued by the Insurance Regulatory and Development Authority of India (IRDAI) to ensure sound and responsive management practices for effective oversight and adequate due diligence with regard to outsourcing of activities by Insurers; and
- Guidelines on Outsourcing of Activities by Intermediaries – issued by the Securities and Exchange Board of India where core business activities such as execution

of orders and monitoring of trading activities of clients in case of stock brokers; dematerialisation of securities in case of depository participants, among others, cannot be outsourced.

Law stated - 8 September 2026

Contractual terms

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

While there is no overarching law governing outsourcing of contract in India, there are multiple sector-specific guidelines and regulations that govern the outsourcing arrangements for regulated entities in India, and that provide for certain standard clauses to be included under such outsourcing arrangements. These include:

- as per the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, issued by Insurance Regulatory and Development Authority of India (IRDAI), the outsourcing arrangements entered into by an insurer with an outsourcing service provider located in India or outside India require clauses in relation to information and asset ownership rights, information technology, data security, guarantee or indemnity from the outsourcing service provider, contingency planning, etc;
- as per the Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators, the outsourcing arrangements that payment system operators enter into with third-party service providers should include provisions for scope of services, charges for services and maintaining confidentiality of customers' data, etc; and
- as per the Guidelines on Outsourcing of Activities by Intermediaries, the outsourcing agreements for intermediaries registered with Securities Exchange Board of India should include provisions for the activities to be outsourced, appropriate service and performance levels, mutual rights, obligations and responsibilities of the intermediary and the third party, indemnity, continuous monitoring and assessment by the intermediary, etc.

Law stated - 8 September 2026

Employee rights

50 | 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?

Broadly, under Indian law, employees have no specific rights when services performed by them are outsourced to a service provider (including consultation or compensation rights) unless they are terminated.

In the event such employees are terminated/retrenched or they are transferred, provisions under the Industrial Disputes Act, 1947 for compensation payable to the employee are triggered. Additionally, there are also state specific Shops and Establishments Acts which will also govern terminated, and stipulate minimum notice requirements.

Law stated - 8 September 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51 | 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?

India has not adopted a comprehensive statute dedicated to the regulation of artificial intelligence (AI) and has thus far favoured a principles-based, innovation-oriented and sector-led approach to AI governance.

The Ministry of Electronics and Information Technology (MeitY), which serves as the nodal ministry for digital governance and AI policy, has repeatedly indicated that many AI-related risks can be addressed through a combination of existing laws, targeted sector-specific interventions, governance standards, and risk-based regulatory mechanisms.

As AI technologies became more sophisticated and increasingly integrated into economic and social activities, concerns relating to algorithmic bias, opacity, privacy, misinformation, accountability, and safety began to occupy a more prominent place within India's policy discourse. This shift was reflected in NITI Aayog's Responsible AI for All framework, released in two parts during 2021. The framework articulated a set of foundational principles intended to guide the responsible development and deployment of AI systems, including fairness, accountability, transparency, explainability, privacy, safety, inclusivity, and human-centric design. While these principles were not legally binding, they established the foundations of India's emerging AI governance architecture and continue to influence subsequent policy and regulatory developments.

The Responsible AI framework did not immediately translate into a dedicated regulatory regime. Instead, over the following years, the Government continued to explore governance approaches through consultations, sector-specific initiatives, technical standards, and policy discussions addressing emerging issues such as AI safety, liability allocation, intellectual property, deepfakes, content authenticity, cybersecurity, and accountability. These developments reflected a growing recognition that while existing legal frameworks provided a degree of protection against AI-related harms, they were not specifically designed to address the novel risks associated with increasingly capable and widely deployed AI systems.

Against this backdrop, the Government initiated a more formal effort to develop a comprehensive governance framework for AI. An Advisory Group was constituted to examine emerging governance challenges and identify an appropriate governance approach for India. Pursuant to this, a sub-committee was established to formulate practical

recommendations on issues relating to AI governance. These recommendations were subsequently published through the Report on AI Governance Guidelines Development, which served as the foundation for the India AI Governance Guidelines issued by MeitY in November 2025.

Building on principles in the aforementioned reports, there exist several sector specific regulations/advisories in this regard, including the following:

- Securities Exchange Board of India (SEBI): Through circulars issued in 2019, SEBI requires reporting of AI and ML applications and systems offered and used by Mutual Funds, market infrastructure institutions and market intermediaries.
- SEBI has recently notified amendments in February 2025, as per which, all regulated entities (REs) are to assume full responsibility for the use of AI and ML technologies, whether developed internally or procured from third parties. REs are required to ensure that AI/ML systems comply with all applicable laws and are responsible for safeguarding the privacy, security, and integrity of investor and stakeholder data, particularly information held in a fiduciary capacity.
- Further, in May 2026, SEBI also issued an advisory highlighting cybersecurity and operational risks arising from emerging AI-driven vulnerability detection tools such as "Mythos" and has constituted a dedicated task force, "cyber-suraksha.ai", to examine AI-related cyber risks in the securities market ecosystem essentially promoting ethical use of AI.
- Reserve Bank of India (RBI): The RBI Governor has highlighted risks relating to use of AI, including introduction of new vulnerabilities, such as increased susceptibility to cyberattacks and data breaches.
- In 2025, the RBI released the FREE-AI Report, providing a governance framework for the responsible adoption of AI by regulated entities in the financial sector. Although non-binding, the Report outlines the RBI's supervisory expectations for AI deployment, balancing innovation with consumer protection, accountability, and financial stability.
- MeitY: Before the introduction of the India AI Governance Guidelines which demonstrate that AI is to be regulated through a principles-based, risk-proportionate and sector-led framework, with governance obligations calibrated according to the nature of the AI use case and the risks it poses rather than the underlying technology, MeitY had also issued an advisory in 2024 providing for due diligence obligations to be undertaken by intermediaries / platforms and seeks to address the Government's concerns with intermediaries and platforms implementing insufficient measures in light of the rapid development and use of AI and machine learning tools / technologies in India. MeitY has also amended the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in 2026 to regulate Synthetic Generated Information (SGI), including realistic AI-generated. The amendments introduce obligations to prevent unlawful synthetic outputs (such as impersonation-based fraud or non-consensual intimate imagery) created using AI, require prominent labelling and provenance tagging of lawful but realistic synthetic content.
-

Indian Computer Emergency Response Team (CERT-In): Emphasising on the principles of transparency and accountability, the CERT-In has issued the '*Technical Guidelines on SBOM/QBOM & CBOM/AIBOM/HBOM*' on July 09, 2025 (Guidelines) for maintenance of Bill of Materials (BOM). These Guidelines introduce a voluntary yet detailed framework for maintaining BOMs across software, hardware, and AI systems. The Artificial Intelligence BOM framework, in particular, requires documentation of AI model components, ranging from data sources and training configurations to ethical declarations and security vulnerabilities. The purpose being to introduce transparency.

- In 2025, CERT-In issued a blueprint recommending measures to strengthen resilience against AI-enabled cyber threats. It outlines governance, vulnerability management, AI-specific security controls, incident response, supply-chain security, and workforce preparedness, and provides a phased implementation roadmap for organisations to adopt AI-aware cybersecurity practices for ethical use of AI.
- Telecom Regulatory Authority of India (TRAI): In July 2023, TRAI published recommendations titled *Leveraging Artificial Intelligence and Big Data in Telecommunication Sector* and has recommended setting up the Artificial Intelligence & Data Authority of India.
- In 2021, NITI Aayog released a report titled '*Principles for Responsible AI*' outlining seven core principles, namely, safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and reinforcement of positive human values, that govern AI. In recent years, several steps have been taken to shape India's AI policy landscape, and India mostly follows a principle based approach for governance of AI.

In fact, even the Supreme Court of India has adopted a cautious approach towards the use of AI in the judicial system. In May 2026, it released draft regulations restricting AI to an assistive role, prohibiting AI-driven adjudication and predictive profiling, and prescribing governance, transparency, audit, cybersecurity and human oversight requirements. Following an incident involving AI-generated fictitious case citations, the Supreme Court also directed the Bar Council of India to examine AI hallucinations and accountability, after which the Bar Council clarified that advocates remain professionally responsible for verifying AI-generated legal research and that AI cannot replace a lawyer's independent judgment.

Therefore, while there is no dedicated legal framework governing AI in India at present, it may be reasonably inferred that the Indian Government intends to regulate AI through a phased and principle-based approach. India currently adopts a light touch approach to AI governance, emphasising voluntary principles, ethical guidelines, and self-regulation over binding legal mandates. Accordingly, increasing sector specific regulations may be expected in the future and compliance with the same is recommended.

Law stated - 8 September 2026

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?

There is no specific law in India governing intellectual property (IP) and artificial intelligence (AI) or machine learning. India currently adopts a light touch approach to AI governance, emphasizing voluntary principles, ethical guidelines, and self-regulation over binding legal mandates. This allows flexibility for innovation while gradually building a foundation for future regulatory interventions.

In November 2025, MeitY released the India AI Governance Guidelines, which provide a comprehensive articulation of AI governance and a clear indication of how AI regulation is expected to evolve in India. The Guidelines identify the use of copyrighted materials for AI training and the legal status of AI-generated outputs as among the most significant unresolved intellectual property issues. The Guidelines acknowledge that existing copyright frameworks do not clearly address questions relating to training data, licensing mechanisms, ownership of AI-generated content, or responsibility for infringing outputs, and indicate that further policy and regulatory work will be required in this area given that the Copyright Act, 1957 currently protects only works authored by humans and does not extend protection to content autonomously generated by AI. This creates a regulatory gap, as the legal status and ownership of AI-generated works remain uncertain under the existing framework.

Consistent with the recommendations of the India AI Governance Guidelines, the Department for Promotion of Industry and Internal Trade (DPIIT) released Part I of its Working Paper on Generative AI and Copyright, titled *One Nation, One License, One Payment*, in December 2025. The Working Paper examines whether India's existing copyright framework adequately addresses the use of copyrighted material for AI training and explores potential approaches to balancing innovation objectives with the interests of copyright owners. After reviewing international approaches, including voluntary licensing, text and data mining (TDM) exceptions, opt-out mechanisms, and collective licensing, the Working Paper proposes a hybrid licensing framework comprising: (1) a blanket license for lawfully accessed copyrighted works for AI training purposes; (2) royalties payable upon commercialisation, with rates determined through a government-supervised rate-setting process; and (3) a centralised Copyright Royalties Collective for AI Training (CRCAT) to administer royalty collection and distribution. While the Working Paper remains a consultative policy document and no legislative amendments have been introduced to implement its recommendations, it represents a significant policy initiative addressing copyright issues arising from AI training.

A recent and significant development in this area is the Delhi High Court's judgment in *ANI Media (P) Ltd. v Open AI Inc.* (CS(COMM) 1028/2024), delivered on 24th July 2026, which represents the first judicial consideration of whether the use of copyrighted works for AI training amounts to infringement under the Copyright Act.

The Delhi High Court framed four key issues for determination: (1) whether storage of copyrighted data for AI training amounts to infringement; (2) whether use of copyrighted data to generate responses amounts to infringement; (3) whether such use qualifies as

fair dealing under Section 52 of the Copyright Act; and (4) whether Indian courts have jurisdiction given that Open AI's servers are located in the United States. The Court appointed two Amici Curiae to assist in examining these novel issues.

In its interim order, the Delhi High Court denied ANI's application for interim injunction. On the output claim, the Court held that the responses generated by ChatGPT were not substantial reproductions of ANI's articles. On the training claim, the Court held, on a prima facie view, that Open AI's storage of ANI's works for training its LLMs fell within "private or personal use, including research" under Section 52(1)(a)(i) of the Copyright Act and satisfied both the purpose test and the fairness test, thereby constituting fair dealing. The Court formulated three factors for determining fairness: (a) whether Open AI's use is limited to training its LLMs; (b) whether such use would result in economic competition or prejudice ANI's legitimate interests; and (c) whether the functions performed by Open AI serve the overall public interest. The Court concluded that all three factors favoured Open AI. The Court also held that balance of convenience and irreparable injury did not favour grant of interim relief, noting that ANI's claim was quantifiable in monetary terms and that an injunction would adversely affect the public interest in AI development.

Accordingly, while there is no law in India regulating the intersection of AI and IP, but it can be presumed that are key issues corresponding to intellectual property that require intervention, and some developments may be seen in the near future. The position in relation to accountability, and the interplay between AI and IP remains untested.

Law stated - 8 September 2026

Ethics

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

At present, there is no comprehensive legislation in India specifically governing the ethical use of Artificial Intelligence (AI). However, various government bodies and policy think tanks, most notably NITI Aayog, have issued guidance documents from time to time that lay down foundational principles for responsible AI development. In 2021, NITI Aayog's report titled '*Principles for Responsible AI*' outlines seven core principles, namely, safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and reinforcement of positive human values. These principles have served as reference points for sectoral regulators such as the Securities Exchange Board of India (SEBI), the Reserve Bank of India, and Ministry of Electronics and Information Technology (MeitY), the Competition Commission of India (CCI) when issuing standards or advisories. We have provided below some examples of developments by these regulators:

MeitY

In 2024, MeitY issued an advisory on the need for transparent labelling in relation to deployment of under-tested or unreliable AI models, including large language models and generative AI.

More recently, in 2025, MeitY released the AI Governance Guidelines, reaffirming a principle-based approach that builds upon and endorses NITI Aayog's earlier Principles for Responsible AI. This approach aligns with international standards such as the European Union Artificial Intelligence Act, which similarly lays down foundational principles for the ethical and trustworthy use of AI. Accordingly, in the absence of a codified legal framework, adherence to these principles and sector-specific advisories should be treated as good governance practice and indicative of the standard of due care expected from entities deploying AI systems in India.

In the same vein, MeitY has also amended the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to regulate Synthetic Generated Information (SGI), including realistic AI-generated. The amendments introduce obligations to prevent unlawful synthetic outputs (such as impersonation-based fraud or non-consensual intimate imagery) created using AI, require prominent labelling and provenance tagging of lawful but realistic synthetic content, and impose enhanced system-level compliance duties on Significant Social Media Intermediaries (including user declarations and pre-publication verification measures) in addition to other compliances. These requirements reflect an ethics-oriented approach centred on transparency, traceability, user awareness and harm mitigation.

SEBI

SEBI, in 2025, amended the Securities and Exchange Board of India (Intermediaries) Regulations, 2008, the Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018, and the SEBI (Depositories and Participants) Regulations, 2018 to require all regulated entities (REs) to assume full responsibility for the use of artificial intelligence (AI) and machine learning (ML) technologies, whether developed internally or procured from third parties. The amendments apply irrespective of the scale, extent, or purpose of AI adoption. REs are required to ensure that AI/ML systems comply with all applicable laws and are responsible for safeguarding the privacy, security, and integrity of investor and stakeholder data, particularly information held in a fiduciary capacity. Further, REs remain liable for all consequences arising from outputs generated by AI/ML systems that are relied upon in the course of their business or for servicing investors.

Further, in May 2026, SEBI also issued an advisory highlighting cybersecurity and operational risks arising from emerging AI-driven vulnerability detection tools such as 'Mythos' and has constituted a dedicated task force, 'cyber-suraksha.ai', to examine AI-related cyber risks in the securities market ecosystem.

RBI

In 2025, the RBI released the FREE-AI Report, providing a governance framework for the responsible adoption of AI by regulated entities in the financial sector. Although non-binding, the Report outlines the RBI's supervisory expectations for AI deployment, balancing innovation with consumer protection, accountability, and financial stability. It identifies key AI risks, including algorithmic bias, lack of explainability, data protection, liability, and systemic risks, and recommends that AI systems be guided by seven principles: trust, fairness, accountability, explainability, human-centric design, safety and resilience, and a pro-innovation approach. The Report also sets out 26 recommendations

across six governance pillars - infrastructure, policy, capacity, governance, protection, and assurance - to support responsible AI adoption.

CCI

In March 2026, the CCI issued a guidance note encouraging enterprises deploying AI systems to undertake voluntary self-audits to identify and mitigate potential competition law risks. The guidance broadly recommends improving transparency in AI-driven decision-making, adopting safeguards against anti-competitive conduct, engaging with stakeholders, promoting interoperable and open-source AI ecosystems, and strengthening regulatory cooperation, among others.

Indian Computer Emergency Response Team (CERT-In): In 2025, CERT-In issued a blueprint recommending measures to strengthen resilience against AI-enabled cyber threats. It outlines governance, vulnerability management, AI-specific security controls, incident response, supply-chain security, and workforce preparedness, and provides a phased implementation roadmap for organisations to adopt AI-aware cybersecurity practices. CERT-In also released voluntary technical guidelines prescribing the maintenance of Software, AI, Hardware, Quantum, and Cryptographic Bills of Materials (BOMs) to improve supply-chain transparency and cybersecurity. Although non-binding, the guidelines are expected to influence industry practices and government procurement expectations. Status: Guidance.

In 2026, CERT-In issued Advisory CIAD-2026-0020 warning that frontier AI models could significantly enhance cyberattack capabilities, including vulnerability discovery, exploit generation, phishing, and autonomous attacks. The advisory recommends strengthening cybersecurity preparedness, continuous monitoring, vulnerability management, and AI risk mitigation frameworks.

In furtherance to regulators framing guidance for the use of AI, the Supreme Court of India (SCI) also released draft regulations in May 2026 governing the use of AI in courts, tribunals and other adjudicatory bodies. The draft limits AI to an assistive role, prohibits AI-driven adjudication and predictive profiling, and prescribes governance, audit, transparency, cybersecurity and disclosure requirements to ensure responsible AI adoption in the judiciary.

Further, following an incident where a trial court relied on AI-generated fictitious judgments, the SCI directed the Bar Council of India to constitute an expert committee to examine AI hallucinations, ethical standards, and verification and accountability requirements for AI-assisted legal work.

The Bar Council of India in June 2026 also went ahead and clarified that advocates must independently verify all AI-generated legal research and remain professionally responsible for any inaccurate or fabricated citations. It emphasised that AI cannot replace a lawyer's independent judgment or ethical obligations to the court and clients.

Thus, while India does not yet have a comprehensive AI-specific legislation, various sector regulators are progressively issuing guidance and frameworks to address the ethical, cybersecurity, and operational risks associated with AI deployment.

Law stated - 8 September 2026

TAXATION

Online sales

- 54** | Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Indian indirect tax laws have undergone a complete overhaul with the introduction of the goods and services tax (GST) with effect from 1 July 2017. As per the Indian GST laws, the supply of all goods and services within India, which, inter alia, includes sale (whether online or offline), barter, exchange and lease, etc, is subject to GST, unless specifically exempted. The import of goods is separately liable to customs duties, a component of which includes GST distinct from the GST payable on supply of goods or services. The rate of such taxes varies depending upon the classification of such goods and their nature.

Separately, in terms of the current GST framework, an e-commerce operator (who owns, operates or manages an e-commerce platform) is required to collect tax at source (TCS), at a rate of 1 per cent on the net value of taxable supplies of goods and services made by the vendors through the e-commerce platform, where the consideration for such supply is to be collected by the e-commerce operator. Further, TCS is to be collected once supply has been made through the e-commerce operator and the business model is such that the consideration is to be collected by the e-commerce operator, irrespective of the actual collection of consideration. The provisions related to TCS under the Indian GST laws were made applicable with effect from 1 October 2018.

Law stated - 8 September 2026

Server placement

- 55** | 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?

Placing of servers within India by an offshore entity could be subject to goods and services tax in India, depending on the specifics of how such server is used in providing services within India or carrying on business in India. Accordingly, the taxability of placing servers within India by an offshore entity needs to be examined in light of specific facts and circumstances.

Law stated - 8 September 2026

Electronic invoicing

- 56** | 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?

The e-invoicing system under the goods and services tax regime was implemented with effect from 1 October 2020 for taxpayers with an aggregate turnover exceeding 5 billion rupees. Subsequently, the e-invoicing requirement was extended to businesses with an aggregate turnover exceeding 1 billion rupees. Thereafter, the Central Board of Indirect Taxes and Customs (CBIC) notified the applicability of the e-invoicing requirement to businesses with an aggregate turnover ranging between 500 million rupees and 1 billion rupees, with effect from 1 April 2021. The government recently extended the applicability of the e-invoicing requirement to businesses having turnover of more than 200 million rupees, with effect from 1 April 2022.

The e-invoicing requirement shall not be applicable to the following categories of registered persons, irrespective of turnover, as notified in the CBIC's Notification No. 13/2020:

- an insurer or a banking company or a financial institution, including a non-financial banking company;
- a goods transport agency;
- a registered person supplying passenger transportation services;
- a registered person supplying services by way of admission to the showing of cinematographic films in multiplex services;
- a Special Economic Zone unit (excluded via CBIC Notification No. 61/2020); and
- a government department and local authority (excluded via CBIC Notification No. 23/2021).

There is no requirement to issue invoice copies in triplicate or duplicate, if e-invoicing is applicable to the taxpayer.

Law stated - 8 September 2026

DISPUTE RESOLUTION

Venues

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

Under the Information Technology Act, 2000 (IT Act), an adjudicating officer, appointed by the central government, is empowered to adjudicate the offences pertaining to contravention of any of the provisions of the IT Act or of any rule or regulation, made thereunder. The IT Act also stipulates that the Telecom Disputes Settlement and Appellate Tribunal established under the Telecom Regulatory Authority of India Act 1997 will be the Appellate Tribunal for the purposes of disputes under the IT Act.

Separately, the Reserve Bank of India has established offices of 'ombudsman' across various locations in India in respect of customer complaints including arising from prepaid instruments, e-wallets and other payment service providers.

Complaints related to online purchases, digital service failures, or e-commerce frauds can be brought before consumer courts under the Consumer Protection Act, 2019.

Further, disputes related to digital contract disputes, online defamation, intellectual property infringement, or data breach claims can be filed in regular civil or criminal courts, depending on the relief sought (damages, injunctions, prosecution).

Law stated - 8 September 2026

ADR

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

There are no specific alternative dispute resolution (ADR) methods available under Indian law specifically in respect of online and digital disputes, however, the regular ADR methods such as arbitration, mediation, conciliation, available under Indian law may be used for online and digital disputes as well.

Given the rise in online and digital disputes in India, the use of ADR methods available under Indian law has also increased.

Law stated - 8 September 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

In India, several emerging regulatory trends are shaping the digital landscape. The Digital Personal Data Protection Act, 2023 (DPDPA), though not yet in force, is set to significantly impact how businesses collect, process, and store personal data, introducing obligations such as user consent, grievance redressal mechanisms, and the appointment of Data Protection Officers for significant data fiduciaries. Separately, as the use of artificial intelligence grows, Indian courts and policymakers are beginning to confront legal questions around copyright, accountability, and bias, with landmark cases like *ANI v OpenAI* highlighting the need for AI-specific regulation. Additionally, the government is advancing digital access

In India, several emerging regulatory trends are shaping the digital landscape. The Digital Personal Data Protection Act, 2023 (DPDPA) along with the rules framed thereunder, which is being implemented in a phased manner and will fully come into force by May 2026, is set to significantly impact how businesses collect, process, and store personal data, introducing obligations such as user consent, grievance redressal mechanisms, and the appointment of Data Protection Officers for significant data fiduciaries. Separately, as the use of artificial intelligence grows, Indian courts and policymakers are beginning to confront legal questions around copyright, accountability, and bias, with landmark

cases like *ANI v OpenAI* highlighting the need for AI-specific regulation. Additionally, the government is advancing digital accessibility standards and making efforts to align with international norms for persons with disability, which are expected to influence both public and private digital platforms. In the cybersecurity domain, the Indian Computer Emergency Response Team released the Comprehensive Cyber Security Audit Policy Guidelines in July 2025, mandating periodic audits for critical infrastructure and digital service providers, and strengthening incident response protocols. These developments collectively signal a more structured regulatory environment for digital transformation and online business in India.

ibility standards and making efforts to align with international norms for persons with disability, which are expected to influence both public and private digital platforms. In the cybersecurity domain, the Indian Computer Emergency Response Team (CERT-In) released the Comprehensive Cyber Security Audit Policy Guidelines in July 2025, mandating periodic audits for critical infrastructure and digital service providers, and strengthening incident response protocols. These developments collectively signal a more structured regulatory environment for digital transformation and online business in India.

Law stated - 8 September 2026



AZB & PARTNERS
ADVOCATES & SOLICITORS

Hardeep Sachdeva
Priyamvada Shenoy
Shagun Badhwar
Nishant Thakur
Sahil Tandon
Amulya Bhatia

hardeep.sachdeva@azbpartners.com
priyamvada.shenoy@azbpartners.com
shagun.badhwar@azbpartners.com
nishant.thakur@azbpartners.com
sahil.tandon@azbpartners.com
amulya.bhatia@azbpartners.com

[AZB & Partners](#)

[Read more from this firm on Lexology](#)

Italy

[Paolo Balboni](#), [Luca Bolognini](#), [Raffaella Cesareo](#), [Luciana Di Vito](#), [Camilla Serraiotto](#), [Claudio Partesotti](#)

[ICT Legal Consulting](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The government has adopted a cognisant approach to internet issues. The complexity and potential of the internet and the challenges it poses must be balanced with the rights and freedom of individuals. With this in mind, Italy's digital transformation strategy highlights the legislature's comprehensive approach from the private sector to public administration. In this context, the government is aware of the need to:

- strengthen the digital culture of citizens and enterprises; and
- improve the online provision of goods and services, which is considered a priority.

Therefore, to implement the beneficial effects of Industry 4.0, enterprises must be provided with digital knowledge-based technology to foster competitiveness. Moreover, the National Recovery and Resilience Plan (PNRR) adopted by Italy is dedicated to the digital transition. The Strategy for Digital Italy develops along two axes: the digitisation of the PA and ultra-fast networks. This approach continues to be reflected in the Digital Italian 2026 strategy, while [the Italian Strategy for Artificial Intelligence 2024–2026](#) confirms the government's focus on AI-driven innovation.

Law stated - 16 September 2026

Legislation

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

There are two main e-commerce models in Italy: business to business (B2B) and business to consumer (B2C), while new models such as consumer to business and consumer to consumer are developing. The legislature has adopted different legal instruments to regulate e-commerce in a comprehensive manner and has provided for the application of special legislation, including:

- [Legislative Decree 70/2003](#), which implements [EU Directive 31/2000/EC](#) with the aim of developing an e-commerce framework;
- [Legislative Decree 206/2005](#) (the Consumer Code) on consumer rights. The Consumer Code has recently undergone important legislative changes, aimed at transposing European standards for greater consumer protection, including some aspects of the sale of goods and the supply of digital content and digital services, respectively contained in [EU Directive 2019/771](#) and [EU Directive 2019/770](#), as further indicated below;
- [Legislative Decree 26/2023](#), implementing [EU Directive 2019/2161](#), which amends the Consumer Code and increases consumer protection;

- [Legislative Decree 28/2023](#), implementing [EU Directive 2020/1828](#), on actions for collective consumer interests.
- EU Directive 2161/2019, implemented through article 4 of the European Delegation Bill, approved by the Italian Senate (AS 2481) on 30 June 2022;
- [Legislative Decree 170 of 4 November 2021](#), implementing EU Directive 2019/771, which amends the Consumer Code as of 1 January 2022; and
- [Legislative Decree 173/2021](#), implementing EU Directive 2019/770, whose provisions (set out in the new Chapter I-bis of Title II of Part IV of the Consumer Code) apply to the supply of digital content or digital services from 1 January 2022, with the exception of the right of redress and the rules on the modification of the digital content or service, which only apply to contracts concluded from that date.

Further, the following laws and regulations apply:

- the regulation of contracts set out in the [Civil Code](#) and the [Digital Administration Code](#) (update by Legislative Decree No. 144/2024) regarding the online signature of contracts;
- [the Personal Data Protection Code](#);
- [EU Regulation 2016/679](#) (General Data Protection Regulation);
- [Legislative Decree 45/2012](#) on electronic money;
- [Digital Services Act](#) (EU Regulation 2022/2065);
- the AI Act (Regulation (EU) 2024/1689) and Law No. 132/2025 on artificial intelligence;
- The Digital Markets Act ([EU Regulation 2022/1925](#)), which governs gatekeepers in digital markets;
- The Data Act (EU [Regulation 2023/2854](#))
- the national provisions of online payment services and intellectual property;
- sector-specific legislation applicable to regulated products and services, including medical products; and

other applicable national sector-specific laws and EU regulations in the areas of cybersecurity, financial services, electronic communications and regulated products.

Law stated - 16 September 2026

Regulatory bodies

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

The main authorities in Italy at this regard are:

- the Competition and Market Authority (AGCM);

- the Communications Regulatory Authority (AGCOM);
- the National Cybersecurity Agency (ACN);
- the Data Protection Authority;
- the Agency for Digital Italy (AgID); and
- sector-specific authorities, including the Bank of Italy, CONSOB, IVASS and ADM.

Law stated - 16 September 2026

Jurisdiction

- 4 | 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?

For international electronic contracts in the European Union, the nature of the parties to a contract determines the application of specific provisions. The general principle for B2B contracts is that parties have a free choice over the applicable jurisdiction of a contract. As a general rule under the recast EU Brussels Regulation (Regulation (EU) No 1215/2012), where the parties have no choice regarding the jurisdiction of a contract, the defendant's jurisdiction will apply, without prejudice to the special jurisdiction rules applicable to contractual matters. Where a defendant is not domiciled in an EU member state, the competent jurisdiction is determined by applicable national law (eg, [Law 218/1995](#) in an Italian context).

If the defendant is a consumer, specific protective rules apply. In these cases, the applicable jurisdiction is the courts of the EU member state in which the consumer is domiciled- unless otherwise agreed- which must follow the EU Brussels Regulation if the parties reside in different countries, or the Consumer Code if they reside in Italy. For digital services concluded online, jurisdiction clauses derogating from the consumer's forum are not valid merely because they are included in online terms and conditions accepted by the consumer. Such clauses are valid only in the cases and under the conditions set out in article 19 of Regulation (EU) No. 1215/2012 (Brussels I bis Regulation) and applicable domestic consumer protection rules, including article 66-bis of the Italian Consumer Code. In the absence of such valid derogation, the consumer may bring proceedings before the courts of their domicile or residence, where applicable.

In the field of telecommunications, the United Sections of the Court of Cassation, in judgments No. 8240 and No. 8241 of 28 April 2020, stated that the failure to carry out the compulsory attempt at conciliation renders the application inadmissible.

Law stated - 16 September 2026

Establishing a business

- 5 | 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?

The regulatory and procedural requirements to establish a digital business in Italy are almost the same as those to establish 'regular' businesses. Operators can choose from different types of business, the most common being limited liability companies and partnerships. There is also a new simplified limited liability company, which was introduced in 2012.

Incorporation must take place before a public notary. Other general requirements to set up businesses include:

- registration with the Register of Companies;
- obtaining a value added tax number;
- obtaining an Economic and Administrative Index number (indicating the category of the activity carried out); and
- certification of the start of the activities and other incumbencies.

Additional requirements for digital businesses include:

- making some corporate and non-corporate information easily accessible (article 7 of Legislative Decree 70/2003); other information instead – according to the rules of the Civil Code – must be included in deeds and correspondence (VAT, registered office, paid-in share capital);
- prior authorisation, if applicable;
- publication of the company's terms and conditions; and

providing details of modalities of payments and other kinds of information to provide transparency regarding the services or products offered.

Law stated - 16 September 2026

CONTRACTING ON THE INTERNET

Contract formation

6 | 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?

The law allows contracts to be signed electronically as part of the 'distance contract' category. The general principles provided by the Civil Code apply to e-contracts. A contract is therefore concluded when one party acknowledges the other party's acceptance of the contract's terms and conditions. An e-contract can be concluded by an exchange of emails. The moment of conclusion in this case is considered to be when an email, containing acceptance of a contract, is delivered to a recipient or inbox of an email service provider. In some cases, the conclusion takes place with the start of the execution of the contract, as e-commerce can often be structured as an offer to the public. E-contracts can be also concluded by a click, which is equal to the signing of a traditional contract (section

1326 of the Civil Code). While 'click-wrap' contracts are valid, on specific unfair clauses jurisprudence has been contradictory on acceptance by the parties with an additional and specific handwritten or strong electronic signature.

Legislative Decree 70/2003 provides that in order for a 'click-wrap' contract to be valid, providers must send confirmation including:

- a summary of the general and specific conditions applicable to the contract;
- details of the main features of the goods or services provided; and
- detailed information regarding the price, payment methods, delivery costs, taxes and the right of the consumer to repent and withdraw, including the terms and conditions to exercise those rights.

It has to be noted that the obligation for the provider to keep available online the versions of the terms and conditions that have succeeded each other over time could refer to the general information obligations laid down in article 5(3) of the Consumer Code.

Article 51 of the Consumer Code also requires that in all distance contracts concluded through digital interfaces, any button or function used to place the order must be clearly labelled 'order with obligation to pay' or equivalent wording, otherwise the contract is not binding on the consumer.

The [Digital Services Act](#) (DSA) has extended the regulation of e-commerce in relation to illegal content, transparent advertising and misinformation. Article 32 of the DSA stipulates that if the platform provider becomes aware that an illegal product or service has been offered through its platform by a trader, it must inform consumers who purchased the illegal product or service in the six months prior to the time it became aware of the illegality.

Furthermore, as part of the tracing obligations of traders under the DSA, the platform provider must carry out verifications with respect to the identification of the third-party seller declaring to be a professional.

Specific obligations related to traceability of traders have been introduced by the DSA. Among others, mention is made of the article 30 of the DSA which requires providers of online platforms allowing consumers to conclude distance contracts with traders to collect some information prior to authorising traders to access to those online platforms (eg, the name, address, telephone number and email address of the trader; the payment account details of the trader; the trade register in which the trader is registered and its registration number or equivalent means of identification in that register; a self-certification by the trader committing to only offer products or services that comply with the applicable rules of Union law). Law No. 214 of 30 December 2023 (Annual Market and Competition Law 2022) introduced two important amendments to the Consumer Code concerning contracts concluded by telephone and the tacit renewal of service contracts.

As EU Directive 2161/2019 has been implemented, providers are also obliged to be more transparent with respect to the parameters for classification of online offers.

Law stated - 16 September 2026

Applicable laws

.

7 | 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?

Legislative Decree 70/2003 is the main framework for contracting on the internet under Italian legislation. The distinction between business-to-business (B2B) and business-to-consumer (B2C) contracts lies in the level of protection guaranteed by the applicable law. Stricter requirements apply in B2C contracts owing to special consumer law provisions (the Consumer Code), under which providers have additional pre-contractual obligations to provide clear and comprehensible information to consumers (sections 1341, 1342, 1325, 1326 and 2702 of the Civil Code).

In B2C contracts, the freedom to choose the governing law and forum is limited by articles 6 and 18–19 of Regulation (EC) No 593/2008 (Rome I) and Regulation (EU) No 1215/2012 (Brussels I bis). As general rule, article 66-ter of the Consumer Code prohibits clauses that, directly or indirectly, waive or restrict consumer rights under national or EU law. Any such clause is null and void unless individually negotiated and expressly accepted.

Regarding the language of the contract, if a website is directed at consumers in Italy, all pre-contractual and contractual information must be provided in Italian, in accordance with article 12 of the Italian Consumer Code and the enforcement practice of the AGCM (Italian Competition Authority). Failure to comply may constitute an unfair commercial practice under articles 20 to 22 of the Consumer Code.

Legislative Decree 26/2023, implementing EU Directive 2161/2019, has introduced relevant amendments, such as:

- new rules on consumers' right to withdraw;
- criteria for identifying the 'previous price' for price reduction notices;
- a requirement for clear information to be provided to consumers in the case of price reductions (any announcement of a price reduction must indicate the lowest price the professional has charged for the sale of the product during the 30 days preceding the application of the reduction);
- the extension of the consumer rights framework to contracts in which the consumer, in exchange for the supply of a digital content or service, provides or undertakes to provide personal data to the professional; and
- individual remedies for consumers (compensation, price reduction, termination of contract, etc) if they are harmed by unfair trade practices.

Legislative Decree 209/2025 updated the Consumer Code rules on distance financial services contracts, including online withdrawal mechanisms.

Legislative Decree 170/2021, implementing EU Directive 2019/771, makes changes to the Consumer Code regarding online sales contracts between consumers and sellers (B2C relationships).

Below are the contents of some of the main provisions, as amended or introduced (sections 128–135-septies of the Consumer Code):

-

conformity of the good must be assessed in light of both subjective and objective requirements;

- the seller is liable for any lack of conformity existing at the time of delivery that becomes evident within two years; and
- complaints for product defects can be made within 26 months of delivery of the good.

The regulation of the supply of digital content and services has been reformed through Legislative Decree 173/2021, which implemented EU Directive 2019/770; the new and amended provisions (set forth in the new Chapter I-bis of Part IV, Title II of the Consumer Code) apply to the supply of digital content and services that takes place on or after 1 January 2022.

The rules of the new Chapter I-bis of the Consumer Code apply to contracts in which the consumer pays a price as well as to those in which the consumer provides or agrees to provide their personal data in exchange for the provision of the digital content or service and such data is not processed for the sole purpose of rendering the service.

Law stated - 16 September 2026

Electronic signatures

- 8** | 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?

E-signatures are regulated by the Digital Administration Code (CAD). The different types of e-signatures recognised by law are simple, advanced, qualified and digital.

While simple electronic signatures (eg, electronic file signed by insertion of username and password, clicking on a tickbox) are considered to satisfy the requirement of written form – although freely assessable in court by a judge – the document signed with an advanced, qualified and digital electronic signature has the evidentiary effectiveness provided for by section 2702 of the Civil Code.

Regulation EU 2024/1183 (eIDAS2) introduces rules on the trust service for the management of devices for the remote creation of electronic signatures or for the remote creation of electronic seals. These rules are relevant, in practice, for qualified trust service providers and for entities using HSMS (Hardware Security Modules) or similar infrastructure for the remote creation of electronic signatures or seals. These requirements have applied since 21 May 2026.

The Agency for [Digital Italy's \(AgID\) Guidelines](#) have been published, which allow for the online signature of documents through the SPID, a public system of digital identification, in compliance with article 20 of the CAD.

It should be noted that the law (article 21 CAD) states that the private deeds referred to in article 1350 of the Italian Civil Code, Nos. 1 to 12, if provided as a digital document, shall be signed, on penalty of invalidity, with a qualified e-signature or digital signature. Furthermore, for public procurement and interactions with the Public Administration, only

qualified or digital signatures are accepted, in compliance with article 65 of the CAD and sector-specific procurement rules.

Law stated - 16 September 2026

Breach

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

For B2C e-contracts, jurisdiction lies with the consumer's domicile, pursuant to article 66-bis of the Consumer Code and Regulation (EU) 1215/2012. Consumers are protected against breaches of pre-contractual obligations, including the imposition of unexpected costs. In cases of lack of conformity, consumers have the right to repair or replacement free of charge, under articles 128 –135-septies of the Consumer Code, as amended by [Legislative Decree 170/2021](#). Pre-contractual liability and general remedies (termination, nullity, damages, price reduction) provided by the Italian Civil Code remain applicable. The EU Online Dispute Resolution (ODR) platform was discontinued as of 20 July 2025; consumer ADR mechanisms remain available under the Consumer Code.

Law stated - 16 September 2026

FINANCIAL SERVICES

Regulation

- 10 | 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?

The promotion and selling of financial services or products are subject to specific rules. Articles 30 to 32 of the [Consolidated Law on Finance](#) regulate the distance selling of financial services or products. The authority for the regulation of the financial markets (CONSOB) has also adopted a specific regulation on intermediaries, which provides that only duly authorised intermediaries can promote and sell financial services or products via distance selling. The Consumer Code provides special protection for consumers.

As of 2 February 2022, asset managers are obliged to comply with the interpretative guidelines issued by the European Securities and Markets Authority, namely, the [Guidelines on Marketing Communications under the Regulation on Cross-Border Distribution of Funds](#), adopted on 27 May 2021.

The Consumer Code rules on distance financial services contracts have been updated by [Legislative Decree 209/2025](#) implementing [Directive \(EU\) 2023/2673](#), strengthening consumer protection in online financial contracts, ensuring clearer pre-contractual information, fair withdrawal terms, and banning misleading interface designs. Additionally, [DORA](#) has applied since 17 January 2025 and imposes digital operational resilience requirements on financial entities, under the supervision of the competent financial supervisory authorities, including the Bank of Italy and CONSOB.

Law stated - 16 September 2026

Electronic money and digital assets

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

Electronic Money Institutions (EMIs) are mainly regulated by [Legislative Decree 218 of December 2017](#), which transposed [EU Directive 2015/2366](#) (PSD2) and came into effect on 13 January 2018.

In Italy, entities other than banks that exclusively carry out the activity of issuing electronic money are called Electronic Money Institutions (IMEIs), empowered to perform this function by EU directives and subject to the supervision of central banks. In Italy, IMEIs are counted among the credit institutions regulated in the [Consolidated Banking Act](#) and are subject to the supervision of the Bank of Italy, which has dictated specific rules of conduct to be followed – for example, the Bank of Italy's Provisions, [dated 22 February 2022](#) and [2 November 2022](#), amending the Supervisory Provisions for Payment Institutions and Electronic Money Institutions of 17 May 2016 (22A01380).

With regard to EU Legislation, reference must be made to [EU Regulation 2023/1114](#) (the Markets in Crypto-Assets Regulation (MiCAR)), which applies to asset-referenced tokens (ARTs) and e-money tokens (EMTs) from 30 June 2024 and has been fully applicable since 30 December 2024. The Regulation establishes uniform requirements for the public issuance of and admission to trading of various crypto-assets.

In Italy, Legislative Decree No. 129 of 5 September 2024 adapted national legislation to MiCAR and designated Consob and the Bank of Italy as the competent national authorities, allocating their respective supervisory powers depending on the type of crypto-asset and activity concerned.

Specifically, the Decree designates the Bank of Italy and the Italian Securities and Exchange Commission (Consob) as the competent national Authorities for supervising crypto-asset activities. In particular, Consob is competent for authorising specialised Crypto-Asset Service Providers (CASPs), subject to the opinion of the Bank of Italy, while supervision over CASPs is shared: Consob focuses on transparency, conduct of business, orderly trading and client protection, whereas the Bank of Italy focuses on risk containment, financial stability and sound and prudent management.

Legislative Decree No. 129/2024 has also introduced specific sanctions for non-compliance with MiCAR provisions, including unauthorised issuance of crypto-assets and provision of services without proper authorisation. The Decree also aligns national legislation with EU standards to ensure effective enforcement.

On 13 September 2024, the Bank of Italy published specific Guidelines for entities intending to issue EMTs or ARTs. In addition, Consob and the Bank of Italy have issued operational indications for applications and notifications under MiCAR.

As of 1 July 2026, the Italian transitional regime applicable for Virtual Asset Service Providers (VASPs) registered with Organismo Agenti e Mediatori (OAM) has expired.

Accordingly, crypto-asset services may now be provided in Italy only by entities duly authorised or otherwise entitled to operate under Regulation (EU) 2023/1114 (MiCAR).

Law stated - 16 September 2026

Digital and crypto wallets

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

Within the European legislative framework, the crypto assets sector is governed by MiCAR, which is fully applicable to member states from 30 December 2024. MiCAR regulates, among other matters, the provision of custody and administration services for crypto-assets on behalf of clients and requires the relevant providers to be authorised, or otherwise entitled to operate, as Crypto-Asset Service Providers (CASPs).

The use of a self-hosted or non-custodial wallet, through which an individual directly controls the relevant private keys or other means of access to the crypto-assets, is not in itself subject to CASP authorisation. However, transfers involving a CASP and a self-hosted wallet are subject to the information, traceability and anti-money laundering requirements laid down in Regulation (EU) 2023/1113 and the applicable Italian anti-money laundering legislation.

In Italy, the [Decree of the Ministry of Economy and Finance dated January 2022](#) established the former national regime applicable to service providers in relation to the use of virtual currencies and digital wallets. Those obligations, however, primarily applied to Virtual Asset Service Providers (VASPs) operating under the national transitional regime preceding the full application of MiCAR. Following the full application of MiCAR and the adoption of Legislative Decree No. 129 of 5 September 2024, the provision of crypto-asset services on a permanent basis is subject to authorisation as a Crypto-Asset Service Provider (CASP) under Regulation (EU) 2023/1114, supervised by Consob and the Bank of Italy according to their respective competences.

Under the former national framework, providers were also required to transmit to the OAM, on a quarterly basis, information concerning their clients and transactions carried out in Italy. Such reporting obligation was extended only up to the information relating to the third quarter of 2025 and no longer forms part of the ongoing reporting framework applicable to authorised CASPs.

Italy has recently updated its regulatory framework for crypto wallets and digital asset services. With Decree-Law No. 95/2025, the government extended the transitional regime for Virtual Asset Service Providers (VASPs) until 30 June 2026. Entities registered with the OAM by 27 December 2024 were allowed to operate legally during this period if they submitted an application to become Crypto-Asset Service Providers (CASPs) by 30 December 2025, in preparation for full MiCAR implementation.

Since the transitional regime expired on 30 June 2026, crypto-asset services in Italy may now be provided only by entities duly authorised or otherwise entitled to operate under MiCAR.

In addition, [Law No. 197 of 29 December 2022](#) (Budget Law 2023, article 1, paragraphs 126 to 147) introduced, for the first time in Italian legislation, a comprehensive tax regime for cryptocurrencies, crypto-assets or virtual currencies. The provision thus introduces a unitary tax regulation for crypto-assets, which includes taxation of capital gains realised and other income received through transactions involving crypto-assets. From 1 January 2025, all capital gains from crypto transactions are now subject to taxation, regardless of the amount. From January 2026, the capital gains tax rate will increase to 33 per cent.

Law stated - 16 September 2026

Electronic payment systems

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

[The EU Payment Services Directive \(2015/2366/EU\) \(PSD2\)](#) aims to improve existing EU standards for electronic payments. The PSD2 sets standards covering security, transparency and information requirements for electronic payments and the protection of consumers' financial data, together with the rights and obligations of users and payment service providers.

The PSD2 introduced the 'open banking' (or 'open data') system, in which financial information is shared, subject to customer consent, between banks and with external companies, as well as 'third parties', to develop innovative products and services.

Italy has implemented the PSD2 via Legislative Decree 218/2017 (also amended by Legislative Decree No. 36/2020). The main changes that the Decree has introduced concern:

- the extension of scope of certain exemptions thereto; and
- the introduction of new payment services to which service providers in this sector are subject.

The recent measures regarding the point of sale (POS) obligation and electronic invoicing contained in the [National Plan of Resilience and Recovery 2](#) came into force in July 2022 in favour of the use of electronic payments. Specifically, an administrative penalty will be linked to the POS obligation, and electronic invoicing will be extended to the flat-rate schemes.

In 2018, the Agency for Digital Italy's (AgID) Guidelines on electronic payments for public administrations and public service providers that adopt AgID's platform were issued. The Guidelines define rules, standards and technical specifications.

Italy has recently strengthened its digital payments framework. Decree No. 1/2024 promotes software-based receipt transmission, and CESOP (Central Electronic System of Payment Information) reporting became mandatory in January 2024 for cross-border transactions. The Bank of Italy reports growing digital payment use and reduced cash reliance.

As directly applicable EU regulations, [DORA](#) and [Regulation \(EU\) 2024/886](#) on instant credit transfers in euro also apply in Italy. DORA has applied since 17 January 2025 and

imposes digital operational resilience requirements on financial entities. Regulation (EU) 2024/886 introduced specific requirements for instant credit transfers in euro, including payee verification.

Law stated - 16 September 2026

Online identity

- 14** | 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?

In Italy, the use of third parties to satisfy KYC and AML identification requirements is permitted, but it is subject to the Anti-Money Laundering Decree ([Legislative Decree No. 231/2007](#)), as amended, sectoral supervisory provisions and EU rules. Reliance on a third party does not transfer responsibility: the obliged entity remains ultimately responsible for customer due diligence, risk assessment, beneficial ownership checks, ongoing monitoring and suspicious transaction reporting.

Italian law allows remote identification where the customer holds a digital identity with at least a substantial assurance level under SPID or another electronic identification scheme notified under article 9 of the [EU Regulation No. 910/2014 \(eIDAS Regulation\)](#). The same framework also supports identification through qualified electronic signature certificates and secure electronic identification procedures authorised or recognised by AgID. In practice, SPID, CIE and qualified trust services may support KYC processes, but they do not replace all AML obligations: the intermediary must still assess the customer risk profile, identify and verify the beneficial owner where applicable, understand the purpose and intended nature of the relationship, conduct sanctions and politically exposed person checks and perform ongoing monitoring.

Where KYC is performed through third parties, the obliged entity must ensure that the third party is itself subject to appropriate AML/CFT obligations and supervision, obtain the relevant identification and verification information immediately, and be able to receive copies of the underlying documents or data without delay. Outsourcing arrangements and agency models must also preserve auditability, data protection compliance, contractual controls, record retention and the possibility for the obliged entity and the competent authorities to access the relevant information.

[The EBA Guidelines on remote customer onboarding](#), applicable from 2 October 2023, are particularly relevant for banks and financial institutions. They require governance over onboarding solutions, pre-implementation assessments, controls over authenticity and integrity of documents and data, fraud and impersonation safeguards, liveness or equivalent checks where used, ICT and data-protection controls, and ongoing review of the solution.

[EU Regulation 2024/1183](#) (eIDAS2) has introduced the European Digital Identity Wallet framework. Member States must provide EU Digital Identity Wallets by the end of 2026, and service providers legally required to identify customers unequivocally will have to accept the wallet according to the applicable implementation timeline. As of July 2026, this is a transition framework: EUDI Wallets and the Italian IT-Wallet ecosystem are expected

to strengthen remote KYC, interoperability and data minimisation, but they should be integrated into, not substituted for, AML customer due diligence.

Finally, the 2024 EU AML package, including [Regulation \(EU\) 2024/1624](#), [Directive \(EU\) 2024/1640](#) and the [AMLA Regulation](#), will further harmonise customer due diligence, digital identification and supervision from 2027. Until then, Italian obliged entities should continue to apply the current national AML framework, EBA guidance and a documented risk-based approach when relying on third parties or digital identity tools.

Law stated - 16 September 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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 '.it' domain is assigned by the Italian Registration Authority (RA) under the [Regulation on Assignment and Management of Domain Names](#) (the Regulations). Applications to register a '.it' domain name must be filed with the RA through a registrar and in accordance with the Regulations. Other restrictions include the prohibition of registering domain names identical or similar to third-party distinctive signs so as to profit from their goodwill or reselling them to such third-party owners (cybersquatting, typosquatting). Italian law and the .it Registry rules also provide for alternative dispute resolution and reassignment procedures that allow trademark owners and other right holders to challenge abusive domain name registrations.

The main principles for domain names are 'first come, first served' and the domain name's uniqueness. According to applicable law, only business entities or adult individuals that are resident or have a registered office in a European Economic Area country, the Vatican State, San Marino or Switzerland may register a domain name in Italy.

The licensing of domain names is not a common business practice in Italy but is legally feasible (usually within the broader scope of trademark licence agreements). Registrars' terms of service might nevertheless require that the domain name owner assumes liability for damages caused by unlawful use of the domain if the owner fails to provide the licensee's contact details to a third party giving reasonable evidence of actionable harm. As a general rule, URLs may be used to direct users to websites, online resources or virtual environments without prior authorisation. However, the use of URLs may give rise to trademark infringement, copyright infringement, unfair competition or misleading commercial practices where the URL creates confusion as to the origin of goods, services or content, exploits the reputation of third-party rights holders, or directs users to unlawful content.

While the [Digital Services Act](#), (Regulation (EU) 2022/2065) does not regulate the registration of domain names, it has strengthened the framework applicable to online intermediaries and platforms in relation to illegal content and online services accessible

through domain names and URLs. No specific Italian rules currently apply to domain names or URLs used to access metaverse environments, and the general principles governing distinctive signs, intellectual property rights and unfair competition continue to apply.

Law stated - 16 September 2026

IP ownership

- 16** | 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?

Domain names are subject to the principle of unity of distinctive signs ([Intellectual Property Code](#), section 22). It is therefore prohibited to adopt a domain name that is identical or similar to a trademark used in a business activity if the similarity between the signs or business activity and the products or services will cause a likelihood of confusion. The owner of a pre-existing trademark may invoke protection based on trademark or unfair competition rules. Likewise, registration of a domain name does not per se imply that that a distinctive sign also fulfils all the requirements for trademark protection.

As a general rule, domain names and URLs are not protected by copyright merely because they have been registered or used online. Copyright protection may arise only in exceptional circumstances where the relevant sign contains sufficiently original and creative elements capable of qualifying as a protected work under copyright law.

Ownership of a registered trademark is usually fundamental to support the claimant's rights against a competitive use or registration of a similar domain name. Indeed, to challenge a '.it' domain name registration, claimants must provide evidence of:

- ownership of a distinctive sign (ie, a trademark or a service mark, a company name, a name) with which the disputed domain name is identical or confusingly similar;
- the absence of legal rights or a legitimate interest of the registrant in the disputed domain name; and
- the domain name having been registered and used in bad faith.

Trademark ownership is therefore often the most effective basis for challenging cybersquatting, typosquatting and other abusive domain name registrations, both before the courts and through the .it domain name reassignment procedures. Copyright may also assist where the disputed domain name incorporates or exploits protected creative content, although such situations are comparatively uncommon in practice.

Law stated - 16 September 2026

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

Online advertising is regulated by national and EU laws, along with self-regulatory codes.

The main legal framework includes:

- The Consumer Code (Legislative Decree 206/2005), which covers misleading and unfair commercial practices;
- [The Personal Data Protection Code](#) and the [EU Regulation 2016/679](#) (General Data Protection Regulation);
- The Digital Services Act ([Regulation \(EU\) 2022/2065](#)), directly applicable since February 2024, which introduces transparency obligations for online platforms, especially regarding advertising and targeting practices;
- The AI Act([Regulation \(EU\) 2024/1689](#)) and [Law No. 132/2025](#) on artificial intelligence, where AI is used to generate or manipulate content used in advertising, including transparency obligations for certain AI-generated or AI-manipulated content and deepfakes;[Guidelines and a Code of Conduct for Influencers](#), which qualify certain influencers as audiovisual service providers and impose rules on transparency and protection of minors;

[The IAP Self-Regulatory Code](#), accepted by the near totality of advertising operators in Italy through subscription to the IAP or standard clauses included in contracts, updated with the [Digital Chart](#) (Oct. 2024) for influencer marketing and social media transparency.

Law stated - 16 September 2026

Targeted advertising and online behavioural advertising

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

As a general rule, consent is required to profile a customer base for targeted advertising, according to article 122 of the Personal Data Protection Code (implementing the EU e-Privacy Directive 2002/58/EC). With regard to cookies, in June 2021 the Italian Data Protection Authority adopted new [Guidelines on the Use of Cookies and Other Tracking Tools](#), which replace the previous guidelines provided by the Authority in 2014. Most importantly, the Guidelines confirm that the prior informed consent of the user referred to in article 122 of the Personal Data Protection Code needs to fulfil the validity requirements set forth in articles 4(11) and 7 of the General Data Protection Regulation, namely, consent must be expressed by means of a clear affirmative action, such as by clicking on a button or ticking a box. Therefore, actions such as scrolling or swiping through a web page, or similar user activity, do not satisfy the requirement of a clear and affirmative action (as indicated by the European Data Protection Board in its Guidelines 05/2020 on Consent under Regulation 2016/679).

In 2025, the Italian Data Protection Authority confirmed through [the Decision dated 4 June 2025](#) its strict approach to cookie banners and consent mechanisms.

Specific rules on targeted advertising are included in the DSA. In particular, providers of online platforms that present advertisements on their online interfaces are required to ensure that the recipient of their service can easily identify the following:

- that the information is an advertisement, including through prominent markings;
- the natural or legal person on whose behalf the advertisement is presented;
- the natural or legal person who paid for the advertisement, if that person is different from the natural or legal person on whose behalf the advertisement is presented; and
- meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

The DSA introduces two new restrictions concerning targeted advertising on online platforms: it prohibits targeted advertising of minors based on profiling, as defined by article 4(4) of the General Data Protection Regulation (GDPR), and targeted advertising based on profiling using special categories of personal data, as defined by article 9(1) of the GDPR.

Law stated - 16 September 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

As a general rule, the provisions on misleading and illegal comparative advertising apply to online advertising. In B2C relationships, misleading advertising is mainly assessed under the rules on unfair commercial practices set out in the Consumer Code, while misleading and unlawful comparative advertising between traders is governed by Legislative Decree 145/2007. Misleading actions and omissions are prohibited, and individuals or organisations may report advertising as misleading to the AGCM. AGCM may impose fines of up to €10 million for national infringements and, in B2B context, fines ranging from €5,000 to €500,000.

In the event of a violation of or non-compliance with the IAP's Self-Regulatory Code of Commercial Communication, including its provisions on misleading advertising, the interested parties can file a report or bring the matter before the competent self-regulatory bodies, and a monitoring committee will then commence an investigation. The report must include details of the alleged violation and relevant documentation should also be provided.

Specific sector regulations issued by the relevant authorities may provide additional provisions (eg, advertising relating to financial services).

In particular, given the proliferation of advertising content published online via video-sharing and social media platforms, AGCOM in January 2024 issued the [Guidelines to regulate influencers' activities](#). In 2025, AGCOM adopted revised [Guidelines and a Code of Conduct for Influencers](#), in order to guarantee transparency of audiovisual commercial communications, protection of minors and users, and compliance with audiovisual media rules.

Law stated - 16 September 2026

Restrictions

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

The advertising of pharmaceuticals is authorised only for non-prescription medicinal products. Under [Legislative Decree 219/2006](#), the advertising of pharmaceuticals must be authorised by the Ministry of Health and advertising on the Internet must include details of such authorisation in addition to other requirements (National System Guidelines of the [Ministry of Health](#)).

For games and betting, a general prohibition on advertising, sponsorship and other promotional communications relating to games or betting with cash winnings apply. AGCOM adopted specific [Guidelines](#) on the application of this prohibition.

There are special rules providing restrictions for certain types of services and products such as alcohol, tobacco, financial services, cosmetics products, food and food supplements. The Regulatory Code of Commercial Communication provides special provisions for the advertising of pharmaceutical products, food supplements, beauty treatments, toys, travel and gaming.

Law stated - 16 September 2026

Direct email marketing

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

The use of automated means (eg, automated calling or communications systems without human intervention or email, fax or text) for marketing purposes is allowed only with the prior consent of the data subjects (ie, the 'opt-in'). Unsolicited marketing is not allowed.

In 2013, the Data Protection Authority issued its [Guidelines on Marketing and Against Spam](#) and introduced the requirement for a unique indication of consent for marketing purposes, providing that selective opt-out has to be guaranteed. Consumers or data subjects can opt out at any time from one or more of the means of marketing communication used by data controllers. Other provisions have been introduced for telemarketing ([Law 5/2018](#)), including the [Public Register of Objections](#), which applies to fixed and mobile telephone numbers. The Italian Data Protection Authority has also approved a [Code of Conduct for telemarketing and teleselling](#), with an accredited monitoring body, which strengthens accountability and compliance requirements across the telemarketing supply chain.

Exceptions to the above-mentioned general rule are as follows: section 130 of the Data Protection Code regulates 'soft spam', which is considered an exception to the opt-in rule regarding promotional emails. If data controllers obtain the electronic contact details of customers in the context of the sale of a product or service, they can use this data for direct marketing of similar products or services, provided that the customers are clearly

and distinctly given the opportunity to object free of charge and in an easy manner to such use of their electronic contact details when collected and on receipt of each additional message when customers have initially agreed to such use.

Law stated - 16 September 2026

ONLINE PUBLISHING

Hosting liability

- 22** | 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?

The [Digital Services Act](#), (DSA), applicable as of January 2024, specifies ISPs' duty of care obligations, integrating detailed rules for the various categories of ISP. With regard to hosting providers, user-friendly notification mechanisms for reporting illegal content are provided for. In addition, under article 8 of the DSA providers of intermediary services (which include 'hosting service') do not have 'a...general obligation to monitor the information which...transmit or store' nor to actively seek facts or circumstances indicating illegal activity.

At national level, AGCOM has been designated as the Digital Services Coordinator for Italy. Since 2024, AGCOM has adopted implementing procedural rules concerning, among other things, trusted flaggers and out-of-court dispute settlement bodies under the DSA.

On the ISP's liability, Italian jurisprudence (Decision 7708/19, Corte di Cassazione, Sez V – Court in Rome, Section XVII Civil, Decision 693/2019) confirms what is stated with regards to the ISP's liability, analyses the profiles of liability including omissions and the distinction between active and passive roles of ISPs. More recently, (Decision 17360/2025, Corte di Cassazione Sez III) the Italian Court of Cassation confirmed that, although there is no general preventive monitoring obligation, a hosting provider may be liable if, after receiving a clear and specific notice of unlawful content, it fails to act promptly to remove it.

In judgment No. 4277/2024 of 13 May 2024, the Italian Council of State, after affirming Google's administrative liability in a case concerning indirect gaming advertising, specified that in this case Google operates as an active hosting provider by means of its paid advertisement services, such as Google Ads. Additionally, it performs indexing and service promotion for third-party content and has an economic interest in the success of such actions (ie, to achieve the control of information and allow its customers to 'optimise their online sales').

Reference is also made to Decision 39763/2021 of the Italian Court of Cassation that clearly established the liability of the platform for copyright infringement. Specifically, the Court ruled that the general liability provisions apply to the active hosting provider (eg, that which carries out the activities of content selection and cataloguing). This would result in damages being recovered by the owner of the infringed copyrights.

Law stated - 16 September 2026

Content liability

- 23** | 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?

If the provider directly delivers the incorrect information or intervenes to modify the content of the information, direct liability profiles may apply. If, on the other hand, the content is uploaded by a third party, it is necessary to verify the effective power of control of the website provider, assessing the circumstances of the case. In line with recent Italian case law, including Decision 17360/2025, Corte di Cassazione Sez III, according to the Italian Court of Cassation, a provider that does not play an active role is not subject to a general preventive monitoring obligation, but may be required to act promptly where it receives a sufficiently specific notice of unlawful content.

It is advisable (but not required by law) to post a notice about the origin of content containing a disclaimer regarding the accuracy or correctness thereof to exclude the website provider's liability for incorrect information and for any consequences resulting from reliance on said content. Furthermore, it is advisable to ensure that the terms and conditions relating to the use of the website include specific contractual provisions that release the provider from liability for incorrect information published on its website. Under article 18 of the DSA, where a provider of hosting services, including online platforms, becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the member state or member states concerned of its suspicion.

The DSA applies to online intermediaries and provides for a liability regime in relation to illegal contents provided by the recipients of the service, which varies for providers according to the type of service they provide. In fact, DSA provides for a distinction between 'mere conduit', 'caching' and 'hosting services' (articles 4–6 of the DSA). It also sets stricter requirements for very large online platforms and search engines (ie, those with more than 45 million monthly users and upwards as provided for in article 33(4) of the DSA).

It is also important to consider that, under article 6 of the DSA; "Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content...for the submission of notices exclusively by electronic means", and

article 26 of the DSA, which states that:

Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following:

1. that the information is an advertisement, including through prominent markings, which might follow standards pursuant to Article 44;

2. the natural or legal person on whose behalf the advertisement is presented
3. the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in point (b);
4. meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.

In the absence of specific regulations on the metaverse, metaverse providers would not be excluded from the above considerations.

With regard to the liability of ISPs, Italian jurisprudence (Decision 7 7708/19, Corte di Cassazione Sez V) distinguishes between hosting providers playing an active role and those playing a passive role. An active hosting provider performs certain operations on content (filtering, indexing, selection, etc), while providers playing a passive role merely provide a technical service.

More recent jurisprudence (Decision 39763/2021, Corte di Cassazione) clearly establishes the liability of the platform for copyright infringement.

Law stated - 16 September 2026

Shutdown and takedown

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

Once an ISP becomes aware of such defamatory material, including through a sufficiently specific notice from the affected party, it shall act immediately to remove the information or to disable access to it.

In fact, according to the Civil Supreme Court, the obligation of removal does not always require a formal warning from authorities, but may arise from any sufficiently specific communication made by any means. Decision 17360/2025 confirmed that failure to act promptly after becoming aware of unlawful third-party content may trigger liability.

Law stated - 16 September 2026

INTELLECTUAL PROPERTY

Data and databases

- 25** | Are data and databases protected by IP rights?

Databases can be protected either as creative (copyrightable) works or as assets created through the investment of resources (even where databases may not be qualified as creative). In the first case, the right holder may take action against unauthorised

reproductions or other uses of its database (including, to an extent, the contents of that database). The second case is regulated by the sui generis rights afforded to database owners, who are entitled to prevent reproductions of their database (in whole or in part, to the extent that the arrangement and structure of the database is copied or used without permission), but this entitlement does not extend to the contents of the databases which, in themselves, may not be eligible for protection. Rights holders of databases can authorise the permanent or temporary reproduction of a database, in full or in part, by any means and in any form.

The [EU Directive on Copyright in the Digital Single Market](#) (Directive (EU) 2019/790), as implemented in Italy by [Legislative Decree No. 177/2021](#), introduced specific exceptions for text and data mining (TDM). One exception applies to research organisations and cultural heritage institutions for scientific research purposes, while a broader exception permits TDM by any user unless rights holders have expressly reserved their rights (opt-out). Recent Italian AI legislation ([Law No. 132/2025](#)) further clarified that reproductions and extractions carried out through AI systems, including generative AI, remain subject to the TDM framework established by Articles 70-ter and 70-quater of the [Italian Copyright Act](#).

In addition, the Data Act introduces rules on access to and use of certain data generated by connected products and services; it does not create proprietary rights over data and applies without prejudice to copyright, database rights and other intellectual property protections.

Law stated - 16 September 2026

Third-party links and content

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

Linking to third-party websites may raise different legal issues and therefore a case-by-case analysis is recommended, particularly where new digital environments (including virtual worlds and metaverse applications) are involved. Simply linking to the homepage of another website is generally permissible. Deep linking (ie, linking directly to a specific page within another website) is also generally lawful. Framing (ie, displaying content from another website within the linking website) may, however, raise copyright concerns where it circumvents technological protection measures or otherwise makes protected content available to a new public without authorisation.

Under EU case law, hyperlinks to content that has been lawfully made freely available online generally do not require the right holder's consent. However, linking to unauthorised content, or linking in circumstances where the operator knows or ought reasonably to know that the content is unlawful, may give rise to liability.

Embedding third-party content may also constitute copyright infringement, trademark infringement or unfair competition where users are unable to identify the original source, are misled as to the origin of the content, or are led to believe that a commercial relationship exists between the relevant websites. The use of third-party trademarks in links or metadata may also create infringement risks.

In addition, online intermediaries and platforms are subject to the obligations set out in the Digital Services Act, where linked or hosted content is unlawful, compliance with applicable notice-and-action and content moderation obligations may be relevant in assessing potential liability. Reviewing the terms of use or linking policies of the target website and obtaining consent where appropriate remains advisable, particularly in relation to framing arrangements, systematic content aggregation, commercial partnerships or the use of protected content.

Law stated - 16 September 2026

- 27** | 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?

Web scraping (including through AI systems) is widely used to quickly and automatically collect significant amounts of data from third-party websites. This can be done for a variety of purposes. Although not illegal in itself, the use of web scraping may involve the risk of infringing intellectual property rights and/or third-party personal data breaching contractual terms of use, infringing database rights or constitute unfair competition.

In particular, the [EU Directive on Copyright in the Digital Single Market](#) allows text and data mining from legally accessible works or materials (a) for scientific research purposes or (b) for other purposes, provided that in such cases the author or other rights holder has not expressed a reservation against such uses (so-called opt-out). These exceptions are reflected in Articles 70-ter and 70-quater of the Italian Copyright Law. In addition, [Law No. 132/2025](#) introduced Article 70-septies of the Italian Copyright Law, clarifying that reproductions and extractions carried out through AI systems, including generative AI systems, remain subject to the text and data mining framework established by Articles 70-ter and 70-quater.

It should also be noted that the AI Act, while not directly regulating the protection of intellectual property, requires providers of certain general-purpose AI models to implement policies aimed at complying with EU copyright law and to make publicly available a sufficiently detailed summary of the content used for training where required by the Regulation. The possibility for rights holders to reserve the use of their content for text and data mining purposes (opt-out) derives from the Copyright in the [Digital Single Market Directive](#) and the corresponding national implementing provisions, rather than from the AI Act itself.

Furthermore, the Data Act (Regulation (EU) 2023/2854), applicable from September 2025, establishes rules on access to and use of certain categories of data generated by connected products and related services. The Data Act does not create proprietary rights in data and applies without prejudice to copyright, database rights, trade secrets and other intellectual property rights.

The above principles should likewise apply to the metaverse, in the current absence of a dedicated discipline.

Law stated - 16 September 2026

Metaverse and online platforms

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

There is currently no dedicated legislation covering the protection of intellectual property rights in a metaverse. Hence, all intellectual property principles need to be adapted by way of interpretation to this new technical and commercial scenario (eg, collecting evidence of an infringement, the scope of licensed rights, jurisdiction and applicable law issues, identification of infringers, enforcement against anonymous users or decentralised platforms, and the assessment of damages).

In practice, particular difficulties may arise in determining whether virtual goods, digital assets, avatars, NFTs or other virtual objects constitute infringing uses of protected trademarks, copyrighted works or databases, as well as in establishing territoriality and the location of infringing acts occurring in virtual environments accessible across multiple jurisdictions.

The absence of a metaverse-specific regime generally means that existing copyright, trademark, database right and unfair competition rules apply. Recent EU digital legislation, including the [AI Act](#) and the [Digital Services Act](#), does not specifically regulate intellectual property rights in the metaverse, but may indirectly affect compliance obligations, content moderation practices and the management of AI-generated or user-generated content within virtual environments.

As a general suggestion, negotiations of new IP contracts should also explicitly address licence rights for metaverse-related usage, including virtual goods, digital twins, avatars, immersive experiences, user-generated content and AI-generated content where relevant.

Law stated - 16 September 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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?

Yes. Exhaustion of rights is a principle that embraces both intellectual and industrial property law and is expressly recognised by both the Italian Industrial Property Code and Italian Copyright Law.

Exhaustion occurs only where the first sale or other transfer of ownership is made by the rights holder or with their consent, in the territory of Italy or in the territory of a member state of the European Union or the European Economic Area.

The application of exhaustion of rights to digital products has also been strongly debated at the EU level. As a general rule, EU copyright law recognises exhaustion in relation to the distribution of tangible copies of protected works, whereas the principle does not normally apply to acts of online making available or communication to the public. By way of example,

the Court of Justice of the European Union (CJEU) has held that the supply of e-books by download does not give rise to exhaustion because it constitutes an act of communication to the public rather than a distribution of a tangible copy. A different approach has been adopted in specific circumstances concerning computer software supplied under perpetual licences, where the CJEU has recognised a form of digital exhaustion.

Likewise, at this early stage of the legal analysis of the metaverse, there would be arguments to dispute that exhaustion applies to digital products placed on a metaverse. The same considerations are likely to apply to virtual goods, digital assets and similar items made available within virtual environments, since their use typically involves online access or making available rather than the transfer of ownership of a tangible copy. The mere placement of a digital product on a metaverse or online platform located in another territory would therefore not normally result in international exhaustion of copyright under Italian or EU law.

Law stated - 16 September 2026

Administrative enforcement

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

The Italian Collecting Society (SIAE) and the Communications Regulatory Authority (AGCOM) are granted surveillance powers to prevent and establish copyright infringement (eg, the authority to access premises and request the disclosure of documents). The SIAE also has investigative powers with regard to suspected value added tax avoidance.

AGCOM can adopt measures against the illicit publication of digital work online, including the power to request the removal of access to websites hosting infringing content or the removal of unlawful content. Administrative fines and criminal proceedings may apply in the case of non-compliance with AGCOM.

Recent developments in the EU regulatory framework, including the Digital Services Act, have further strengthened mechanisms for addressing illegal online content, although the DSA does not itself create new intellectual property-specific enforcement powers.

Pursuant to [EU Regulation 608/2013](#) concerning the enforcement of IP rights, Customs can seize goods in the case of IP infringement.

Public prosecutors also have enforcement powers when an IP infringement constitutes a criminal offence. In particular, where criminal offences are suspected, prosecutors and judicial police may carry out searches and seizures, including unannounced inspections comparable to dawn raids.

In addition, Italian courts may grant a range of interim measures in intellectual property disputes, including orders for description, seizure of infringing goods and evidence, preliminary injunctions and other urgent measures aimed at preserving assets or evidence pending the outcome of proceedings. Such measures are judicial rather than administrative in nature.

Administrative authorities do not generally have the power to issue freezing injunctions over a defendant's assets; such measures, where available, are typically granted by the competent courts.

Law stated - 16 September 2026

Civil remedies

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

IP owners can rely on a significant variety of remedies in civil proceedings, either in the course of proceedings on the merits or in urgent actions (interim proceedings). Civil remedies include:

- permanent (and interim) injunctions against infringers;
- penalties for further infringements;
- damages;
- the seizure or destruction of infringing goods or production facilities;
- the publication of a court order;
- the removal of infringing goods from the market; and
- the issue of a disclosure order; and
- orders for the description of allegedly infringing goods, processes, documents and other evidence, which are commonly used to preserve and collect evidence.

Italian courts may also grant precautionary seizure measures in relation to infringing goods and evidence. In addition, general civil law remedies, including conservatory seizure orders, may be available in appropriate circumstances to preserve assets pending judgment.

Law stated - 16 September 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

32 | 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 Code reflects the definition of 'personal data' provided by article 4(1) of the EU General Data Protection Regulation (GDPR):

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 9(1) of the General Data Protection Regulation (GDPR) also introduces special categories of personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership. Genetic data and biometric data are also included as special categories. According to section 2-septies of the Personal Data Protection Code, the Data Protection Authority will adopt specific identification security measures with regard to the selective access to data to ensure that said information is made available to data subjects. The Data Protection Authority has provided specific provisions for the storage and security of genetic data as per Order No. 146/2019, as amended by Order No 66/2025.

Law stated - 16 September 2026

Registration and appointment of data protection officer

- 33** | 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?

There are no registration requirements at present. Where a data protection officer is appointed under GDPR – in house or external -, the controller or processor must communicate the DPO's contact details to the Data Protection Authority, and keep such information up to date, in accordance with article 37(7) of the GDPR.

Law stated - 16 September 2026

Extraterritorial issues

- 34** | 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?

In this respect, Italian data protection legislation follows the rules set out in the GDPR.

Law stated - 16 September 2026

Bases for processing

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

In this respect, Italian data protection legislation follows the rules set out in the GDPR.

Law stated - 16 September 2026

Data export and data sovereignty

- 36** | 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?

In this respect, Italian data protection legislation follows the rules set out in the GDPR. In addition to this are the [Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data](#), which provide for a six-step methodology to address data transfers, and [Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures](#), which summarise the requirements set forth by EU law in order for public surveillance measures to be lawful. In addition, in June 2025, following public consultation, the European Data Protection Board adopted the final version of its Guidelines 02/2024 on Article 48 GDPR, which clarify the conditions under which controllers and processors may lawfully respond to requests for personal data from third-country authorities.

There is no general obligation under Italian law to store personal data in Italy or in the EEA. However, transfers of personal data to third countries remain subject to Chapter V of the GDPR.

In the criminal sector, Italy has adopted [Legislative Decree 51/2018](#), implementing Directive (EU) 2016/680 and repealing Council Framework Decision 2008/977/GAI. Article 31 et seq of the Decree regulates in what cases the transfer of these types of data to a third country or international organisation can take place.

Law stated - 16 September 2026

Sale of data to third parties

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

Particular attention must be paid to cases in which:

- personal data is communicated to autonomous third-party data controllers; and
- lists from third parties are received from autonomous data controllers; it should be verified that personal data has been lawfully collected by the transferor.

In this regard, we refer to the Authority's Guidelines on Marketing and Against Spam (4 July 2013) that provide specific provisions for the transfer of personal data to third parties for marketing purposes. In particular, the Guidelines state that:

a data controller planning to collect personal data also with a view to communicate (or transfer) such data to third parties for the third parties' marketing purposes must first inform data subjects appropriately...and obtain specific consent.

Further, the Data Protection Authority requires that data controllers who intend to use personal data collected or sold by data brokers or third parties must carry out and document adequate verification of the provenance, lawfulness, and consent relating to such data (eg, ensuring that data subjects were duly informed and have explicitly consented to the communication to third parties for marketing). While earlier guidance referred to a 10–15 per cent sample check, current practice no longer fixes a numerical quota, instead requiring a risk-based, provable verification process in line with recent enforcement trends and GDPR accountability obligations.

There is currently no specific metaverse legislation in Italy differing from the applicable industry regulations.

Law stated - 16 September 2026

Consumer redress

38 | 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?

Italian data protection legislation follows the rules set out in the GDPR. In addition, there is no difference between citizens and foreign individuals with regard to data protection law.

Regarding remedies, section 140-bis of the Personal Data Protection Code provides for alternative forms of protection: in situations where data subjects consider that their rights based on the applicable law have been violated, they may lodge a complaint with the Data Protection Authority or appeal before the Italian judicial authority. However, the Italian legislator has prescribed that there are two remedies, mutually exclusive to each other: filing a complaint with the Data Protection Authority or taking the matter to the judicial authority.

Section 141 of the Personal Data Protection Code provides that a data subject may lodge a complaint with the Data Protection Authority, according to article 77 of the GDPR.

The complaint to the Data Protection Authority must contain all the details set out in section 142 of the Personal Data Protection Code (eg, a detailed indication of the circumstances on which it is based and the provisions violated).

Section 144 of the Personal Data Protection Code provides that anyone may submit a report, which the Data Protection Authority may take into consideration.

The Data Protection Authority may take the measures referred to in articles 58 and 56 of the GDPR.

Italian legislation does not provide specific regulations for individuals of Italian citizenship, and the requirements of the GDPR will be applicable.

Law stated - 16 September 2026

Non-personal data

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

Data that is not included within the definition of personal data is regulated by [EU Regulation 2018/1807](#) on a framework for the free flow of non-personal data in the EU. The Data Act, which applies from 12 September 2025, also sets out rules on access to and use of data, including non-personal data generated by connected products and related services.

Law stated - 16 September 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

In January 2022, the new [AgID Guidelines on the Formation, Management and Preservation of Electronic Documents](#) came into effect. The Guidelines apply to all organisations, public and private, obliged to preserve electronic files that constitute the originals to be archived, according to civil, tax and digital administrative obligations.

[Decree 58/2013 of the President of the Council of Ministers](#) identifies the types of unique original analogue documents for which, due to public needs, the obligation to preserve the original documents in paper format remains or, in the case of substitute digital preservation, their conformity with the original must be authenticated by a notary or another authorised public official. Such documents are, for example, and by way of non-exhaustive list: acts contained in the Official Compendium of Legislative Acts of the Republic of Italy; notary acts; judicial, procedural and judicial police acts for the next 20 years; state property and historical documents; and acts preserved in notary archives. The complete list is contained in the [Annex](#) to the aforementioned Decree.

Law stated - 16 September 2026

Retention

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

Italian sector-specific laws provide for the retention period of certain documents.

In some cases, the retention period of documents is determined by the limitation period of legal action: article 2946 of the Civil Code provides that 'except where the law provides otherwise, rights are extinguished by prescription with the lapse of ten years'.

The following are some examples of such sector-specific provisions:

- accounting records must be kept for 10 years from the date of the last entry, pursuant to article 2220 of the Civil Code; and
- tax invoices must be kept for a period of 10 years after their creation.

Law stated - 16 September 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

In Italy, companies must adopt technical and organisational measures proportionate to the nature of their activities, the data processed and the risks affecting networks, information systems, communications, online transactions and payment information. The legal framework is now mainly composed of the GDPR, the Italian implementation of [Network and Information Security Directive](#) (NIS2), National Cybersecurity Perimeter Law ([Law No. 133/2019](#)) rules, the [Digital Operational Resilience Act](#) (DORA) for the financial sector, the [European Union's Payment Services Directive 2](#) (PSD2) for payment services and sector-specific guidance issued by competent authorities.

Under the GDPR, controllers and processors must implement appropriate security measures, including, where suitable, encryption, pseudonymisation, confidentiality, integrity, availability and resilience of systems, backup and restoration capabilities, and regular testing of security controls. The approach is risk-based and must be documented. In the event of a personal data breach, controllers must notify the Italian Data Protection Authority without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk to individuals; affected individuals must also be informed without undue delay where the breach is likely to result in a high risk.

The former NIS framework has been replaced and expanded by Legislative Decree No. 138/2024, which implements NIS2 in Italy and has been in force since 16 October 2024.

The National Cybersecurity Agency (ACN) acts as the competent NIS authority, single point of contact and CSIRT Italia (Computer Security Incident Response Team). Essential and important entities must adopt cybersecurity risk-management measures and notify significant incidents. ACN has issued basic specifications for the first application phase: as of 2026, NIS entities are expected to comply with incident notification requirements and to complete the adoption of the basic security measures according to the applicable statutory timeline, including the October 2026 deadline for entities included in the 2025 list.

The National Cybersecurity Perimeter rules also remain relevant for entities included in the perimeter and require additional controls for ICT assets supporting essential State functions and services, including incident reporting, security measures and controls over certain ICT procurement. Law No. 90/2024 further strengthens the national cybersecurity framework, especially for public administrations and strategic entities.

For financial entities, DORA has applied since 17 January 2025 and requires an ICT risk-management framework, classification and reporting of major ICT-related incidents, digital operational resilience testing, management of ICT third-party risk, contractual controls and, for critical ICT third-party providers, EU-level oversight. For payment services, PSD2 remains the operative framework for strong customer authentication and secure communication, although [PSD3 and the Payment Services Regulation](#) are progressing through the EU legislative process and should be monitored.

Commonly used standards include ISO/IEC 27001 and ISO/IEC 27002 for information security management and controls, ISO/IEC 27701 for privacy information management, ISO 22301 for business continuity, PCI-DSS for payment card data, and the NIST Cybersecurity Framework, including its current 2.0 version. In practice, Italian companies generally rely on a combination of risk assessments, access controls, multi-factor authentication, encryption, secure software development, vulnerability management, logging and monitoring, incident response procedures, employee training, supplier security controls and periodic audits.

Law stated - 16 September 2026

Data breach notification

- 43** | 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?

Italy's data breach notification requirements reflect those set out in the GDPR. The Italian Data Protection Authority has provided a [specific telematic procedure for breach notification in Italian language](#). With regard to cybersecurity incidents, Legislative Decree No. 138/2024, implementing Directive (EU) 2022/2555 (NIS2), has replaced [Legislative Decree 65/2018](#) (implementing EU Directive 2016/1148/EU (the NIS Directive)). The new framework applies to essential and important entities, including certain digital infrastructure and digital service providers, and provides for cybersecurity risk-management and incident notification obligations.

In the case of a significant incident, essential and important entities must notify CSIRT Italia (Computer Security Incident Response Team) without undue delay, in accordance with the procedures and deadlines set out under [Legislative Decree No. 138/2024](#) and the implementing guidance issued by the National Cybersecurity Agency.

Law stated - 16 September 2026

Government interception

.

44 | 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?

In Italy, investigating authorities have the right to access personal data in the course of a criminal investigation.

In particular, under articles 234 and 234-bis of the [Code of Criminal Procedure](#), the judicial police or the Public Prosecutor may obtain copies of acts and documents containing personal data; in the event of a request for data or documents by the judicial authority, it is not permitted to refuse to produce them.

According to article 391-bis et seq of the Code of Criminal Procedure, the defendant's lawyer is allowed, when carrying out defensive investigations, to request personal data. There is no explicit provision for access to acts and documents; the same purpose is achieved by requesting information orally from the person who will be required to answer during the specific interrogation.

Moreover, pursuant to section 132, paragraph 3 of the Personal Data Protection Code, if there is sufficient evidence of crimes for which the law establishes the penalty of life imprisonment or imprisonment of not less than a maximum of three years, and of crimes of threatening and harassing or disturbing persons by means of a telephone, when they are serious, where they are relevant to the continuation of the investigation, the data is acquired from the supplier by reasoned decree of the judge, at the request of the public prosecutor or at the request of the defence counsel of the accused, the person under investigation, the injured party or other private parties. If the prosecutor's decree is not validated within 48 hours, the data acquired cannot be used.

Requests from third-country authorities should also be assessed in light of article 48 GDPR and the [EDPB Guidelines 02/2024](#), adopted in final version in June 2025.

Law stated - 16 September 2026

GAMING

Legality and regulation

45 | 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?

Italy has adopted stringent legislation with regard to online betting and gaming. As a general rule, betting and gaming are governed by the state (through article 1 of [Legislative Decree 496/1948](#)), which can grant concessions to private operators. The new [Legislative Decree No.41 dated 25 March 2024](#) determines significant reforms to remote gaming concessions, particularly in terms of price and duration, strengthening transparency, traceability of gambling money flows, respect for free competition in the common market. Following this reform, the Customs and Monopolies Agency (ADM) launched the new tender procedure for remote gaming concessions under article 6 of the beforementioned Decree, with the award decision published in September 2025

In addition, it provides for very strict requirements for the eligibility of operators and strong restrictions on so-called skin/white-label sites, as each operator must have a website with an Italian domain name and display its logo on the site. Secondary legislation concerning betting and gaming is found in the Civil Code and special laws and regulations issued by the ADM. Different products are regulated separately under the scope of specific laws and regulations (eg, online betting and online bingo). Concessions, authorisations and licences are required to lawfully perform online betting and gaming activities and provide products and services to persons located in Italy. The main type of licence is a concession, which is normally issued through a public tender. The general principle is that only authorised operators can offer online betting and gaming.

Residents can use only licensed online casinos and betting websites. Websites that provide gaming services must indicate that they are authorised to do so. Article 24 of [Law 111/2011](#) prohibits minors (ie, residents aged under 18) from taking part in public games with cash prizes.

Law stated - 16 September 2026

Cross-border gaming

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

According to [Italian gambling advertising guidelines](#) issued by the Authority for Communications Guarantees in 2019, article 9 establishes that the general prohibition of paid game advertising applies to entities having their registered office, including branch offices, in Italy. The provision sets the fight against gambling as a general objective by introducing an absolute ban on the dissemination of 'any form of advertising, including indirect advertising' relating to games with cash prizes presented 'in any form and by any means, including sporting, cultural or artistic events, television or radio broadcasts, daily and periodical press, publications in general, posters and computer, digital and telematic channels, including social media'. The prohibition also applies to entities with registered offices abroad, if they have:

- received a concession for the provision of pay-per-click gaming in Italy from the Customs and Monopolies Agency; and
- been authorised to provide audio-visual media services in Italy.

Distinctive signs of legal gaming are not covered by the prohibition in article 9 only where they strictly identify the place where the relevant activity is carried out (by way of example, mere business signs or domains of online sites).

There is currently no specific metaverse legislation in Italy that differs from the applicable industry regulations.

Law stated - 16 September 2026

OUTSOURCING

Key legal issues

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

There is no overarching legislation on outsourcing, but sector-specific laws and guidelines apply at national level, depending on the type of outsourced service and the sector in which the customer operates. In particular, the Civil Code's general provisions on contracts apply, and its specific provisions on service and work contracts or supply contracts. Hence, the general rules provided in the Civil Code apply with specific regard to the general principles applicable to contracts (article 1321 et seq Civil Code), supply contracts (article 1559 et seq Civil Code) and works and services contracts (article 1655 et seq Civil Code). For IT outsourcing, it should also be considered that recent changes in sector-specific regulation may introduce additional requirements, particularly in relation to cybersecurity, data protection, cloud services, digital operational resilience and, where relevant, artificial intelligence. Sector-specific issues.

Law stated - 16 September 2026

Sector-specific issues

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

Italian law does not provide for a general list of digital business services or core business activities that cannot be outsourced. However, outsourcing arrangements must be structured as genuine service arrangements and should not result in unlawful staff leasing or the mere provision of personnel.

Specific restrictions and regulatory requirements may apply in regulated sectors. For example, in the banking and financial sector, outsourcing is subject to supervisory rules, including those issued by the Bank of Italy, the EBA framework and, where relevant, DORA, particularly for critical or important functions and ICT services. In the public sector, activities involving the exercise of public authority cannot generally be outsourced, while service contracts are subject to public procurement rules. In the healthcare sector, core clinical activities remain subject to sector-specific regulation and authorisations, although ancillary and support services may be outsourced subject to applicable requirements.

Law stated - 16 September 2026

Contractual terms

- 49** | Does the law require any particular terms to be included in outsourcing contracts?

Sector-specific laws and guidelines apply to outsourcing contracts. Among the sector-specific laws, reference is made in particular to:

- EU General Data Protection Regulation (GDPR) (eg, for IT and cloud services);
- CAD: Digital Administration Code;
- Public Procurement Code ([Legislative Decree 36/2023](#))
- the discipline of temporary employment agency work contracts;
- Sub-Supplier Contract Law ([Law 192/1998](#));
- the Bank of Italy's guidelines; and
- circulars governing the outsourcing of services by banking institutions.
- DORA, for ICT third-party risk management in the financial sector;
 - Legislative Decree No. 138/2024 implementing NIS2, for essential and important entities;
 - the Data Act, in particular for data processing services, cloud switching and portability; and
 - the AI Act and Law No. 132/2025, where outsourced services involve AI systems.

In light of the above, it is highly recommended to include some of the following safeguards and mechanisms in outsourcing contracts, as appropriate:

- service levels (SLAs) are usually agreed upon to monitor contract performance and ensure a minimum satisfactory level of service. Other SLA-related remedies may include termination (eg, if a penalty cap is exceeded) and the right to claim compensation for additional damages;
- a detailed change request procedure is usually agreed upon;
- the parties can agree on periodic audits in order to monitor contracts;
- the appointment of joint committees to handle any service-related issues or any changes to the service;
- escalation procedures aimed at involving an adequate level of management to address and manage contractual disputes before a claim is brought to court;
- the adoption of bench marking mechanisms to facilitate the measurement of service performance and agree on service changes or price adjustments (or both); and
- with specific regard to IT outsourcing, in addition to any data processing agreement required under article 28 GDPR, contracts may need to address broader information security, business continuity, disaster recovery, audit, exit, portability and transition obligations, particularly where cloud services or sector-specific regulatory requirements are involved.

Law stated - 16 September 2026

Employee rights

- 50** | 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?

As a general principle, in the case of a transfer of a business, employment relationships are transferred to transferees as a going concern – without the prior consent of employees – and continue seamlessly with transferees. Legislation and case law distinguish between transfers that include the transfer of all assets (ie, workforce, contracts and goods) from transfers that involve a change of supplier that provides services via outsourcing.

Employee rights in the transfer of a business are regulated by section 2112 of the Civil Code. As a general principle, transferred employees maintain the rights from their previous employment relationship. Further, under certain conditions (eg, the number of employees involved), the parties to a transfer must undertake a consultation procedure with trade unions. Where outsourcing is not qualified as a transfer of business, the transferee may decide to apply the Collective Labour Agreement as provided by law to the transfer of employees. The transferee would then commence negotiations with the trade unions.

In the case of outsourcing contracts under which the direct management and implementation of one or more services are carried out by third parties, [Legislative Decree 276/2003](#) provides that third parties and companies requesting the services of a third party are jointly liable for the remuneration, social security and severance package of workers involved in the contract's execution. Recent amendments in 2024 to Legislative Decree 276/2003 have also strengthened certain protections for workers employed under procurement and subcontracting arrangements.

The level of protection guaranteed in Italy depends on whether workers are employees, self-employed or freelance workers.

Law stated - 16 September 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

Italy, as an EU member state, is required to comply with [Regulation \(EU\) 1689/2024](#) (AI Act), adopted on 13 June 2024 which entered into force on 1 August 2024 and applies progressively.

At national level, [Law No. 132/2025](#) on artificial intelligence has been adopted and must be interpreted and applied in accordance with the AI Act. The law sets out national principles for the research, experimentation, development, adoption and application of AI systems and models, promoting a correct, transparent, responsible and human-centric use of AI.

Where automated decision-making or profiling involves the processing of personal data, the GDPR – according to [the article 29 Working Party's Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679](#) – and the Italian Personal Data Protection Code apply. In particular, article 22 GDPR restricts decisions based solely on automated processing, including profiling, where they produce legal effects or

similarly significant effects on individuals, unless one of the exceptions under article 22(2) GDPR applies and suitable safeguards are implemented, including the right to obtain human intervention, express one's point of view and contest the decision. Controllers must also comply with transparency obligations under articles 13 and 14 GDPR and, where applicable, provide meaningful information about the logic involved and the envisaged consequences of the processing.

The Italian Data Protection Authority has issued the [Guidelines on the Processing of Personal Data for Online Profiling – 19 March 2015](#), as well as specific [guidelines on online profiling](#), which confirm that consent is generally required for profiling. These rules are particularly relevant where AI or machine-learning systems are used to profile individuals or support automated decision-making.

In Italy, national rules on automated decision-making in the workplace are found in [Legislative Decree 104/2022](#) (the Transparency Decree), amended by [Legislative Decree 48/2023](#). These require employers to provide clear information on fully automated systems used in recruitment, task assignment, performance monitoring, and employment termination.

In the employment context, recent Italian Data Protection Authority practice ([Order No 667/2024](#)) has also stressed the need to provide clear information on the logic and functioning of fully automated decision-making or monitoring systems, the categories of data and main parameters used, the control measures adopted, and the accuracy, robustness, cybersecurity and potential discriminatory impacts of such systems.

Relevant Italian case law includes:

- Two key administrative decisions (the Regional Administrative Court ([TAR Lazio – Roma, Decision No. 9230/2018](#)) and the Council of State ([Decision No. 8472/2019](#)), which set limits on the use of automated systems in public procedures, stressing:
 - full transparency of the algorithm and
 - the public administration's accountability for algorithmic decisions.
- The Supreme Court of Cassation (Judgment No. 14381/2021), which ruled that valid consent for profiling requires that data subjects clearly understand the algorithm's logic. Consent is not valid if the algorithm's functioning remains opaque.

A data protection impact assessment (DPIA) may be required under article 35 GDPR where processing is likely to result in a high risk to individuals' rights and freedoms, for example due to systematic and extensive evaluation of personal aspects, profiling, automated decision-making or large-scale processing. This assessment may therefore be required in connection with AI-based processing where the relevant use case presents such high-risk features. In 2026, the EDPB also adopted a draft DPIA template for public consultation to support greater consistency in DPIA reporting.

With regard to deployers of certain "high-risk" AI systems- referred to in points 5 (b) and (c) of Annex III of the AI Act- the AI Act requires, under certain circumstances, the implementation of a Fundamental Rights Impact Assessment (FRIA) before deployment.

At EU level, the [Digital Omnibus Proposal](#) published in November 2025 should also be monitored, as it includes proposed targeted amendments to the GDPR and other digital legislation, including provisions relevant to AI-related processing.

Law stated - 16 September 2026

IP rights

- 52** | 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?

The Italian legal framework for Intellectual Property (IP) and Artificial Intelligence (AI) is fragmented, relying on the integration of the AI Act with national laws.

[Law No. 132/2025](#) is the primary recent local development, implementing AI Act principles and clarifying copyright issues without creating a separate regime. As for the rest, AI Act implications must be interpreted in conjunction with existing national and international IP legislation, including [Law No. 633/1941 \(Italian Copyright Law\)](#), the [Legislative Decree No. 30/2005 \(Italian Industrial Property Code\)](#), the Directive (EU) 2019/790 concerning the EU Copyright in the [Digital Single Market Directive](#) (Digital Single Market Directive), implemented in Italy by Legislative Decree No. 177/2021, and other applicable EU legislation.

With regard to AI and Machine Learning, current regulations emphasize transparency and compliance with the Digital Single Market. General-Purpose AI (GPAI) providers must summarise training content using EU-published templates to assist right holders in enforcing their rights. Furthermore, article 70-septies of the Italian Copyright Law specifies that AI training remains subject to existing copyright frameworks, including: (i) the requirement of lawful access to the source material; and (ii) the right of right-holders to reserve their rights and opt-out of TDM uses. AI model providers must therefore respect and implement such reservations where validly expressed. Notably, article 171-ter introduces criminal sanctions for the unauthorised extraction or use of protected content through AI systems.

Training datasets and associated data are protected under exclusive reproduction and extraction rights. Their use is primarily governed by Text and Data Mining (TDM) exceptions (articles 70-ter and 70-quater):

Research/Cultural Institutions may perform TDM for scientific research if they have lawful access.

Commercial Developers may rely on TDM exceptions provided they have lawful access and the right holders have not exercised a machine-readable "opt-out".

Significant uncertainty remains regarding the legality of web scraping, the long-term retention of training corpora, and whether Large Language Model (LLM) training fits entirely within TDM exceptions. Where patent disclosure is not possible, trade secret law serves as an alternative for protecting proprietary data.

Ownership of AI-Generated IP Italy maintains a strictly human-centered approach to IP ownership. AI systems do not have legal personality and cannot hold intellectual property rights or be registered as IP rights owners under current Italian legislation.

[Law No. 132/2025](#) expressly confirms that protection to copyrights is reserved for works resulting from human intellectual creation. AI must remain ancillary or instrumental; purely AI-generated works are not recognised.

With regards to patents an inventor must be a natural person. AI cannot be designated as an inventor in patent applications. For AI-assisted inventions, a human must actively define the technical problem, select parameters, or validate results. Detailed logs of human-AI interaction are essential to prove human inventorship. Inventions created by employees using corporate AI tools generally belong to the employer.

About designs, AI systems themselves cannot own design rights. EU and Italian design law generally does not expressly require human authorship as a condition for obtaining design protection. The protection requirements are the same as those applied to industrial designs created without the use of AI: novelty and individual character. In assessing these requirements, the fact that the design was created with the aid of AI is essentially irrelevant.

About trademark, there is currently no prohibition on registering a trademark simply because AI was involved in its creation provided that the legal requirements for trademark registration (novelty, distinctiveness, lawfulness) are met. Ownership of the resulting trademark rights lie with the natural or legal person who files the application and uses the sign in trade, not with the AI system.

Law stated - 16 September 2026

Ethics

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

At international level, relevant references include the [OECD's Recommendation of the Council on Artificial Intelligence](#) - amended in 2024 - and various guidelines on AI in medicine. In May 2025, the ISO published ISO/IEC 42005:2025, which provides guidance for conducting AI impact assessments, helping organisations evaluate the social and individual effects of AI systems and ensure transparency and accountability throughout their lifecycle.

After the publication of the AI Act in the EU Official Journal, Italy's Department for Digital Transformation released in 2024 [the Italian Strategy for Artificial Intelligence 2024–2026](#), which remains the main national policy framework for AI priorities across research, public administration, business and training. The strategy balances innovation with the ethical implications arising from the use of AI systems.

[Law No. 132/2025](#) on artificial intelligence has introduced principles for the research, experimentation, development, adoption and application of AI systems and models. The law promotes a correct, transparent and responsible use of AI in a human-centric

dimension and requires attention to the economic and social risks, as well as the impact on fundamental rights, arising from AI.

Additional national initiatives include the National Research Programme 2021-2027, which dedicates specific focus to AI and its integration with cybersecurity, robotics, and big data and the AI Ethical Lab-EL, launched under the National Innovation Plan 2025, which brings together public and private actors to define ethical-legal standards and criteria for qualifying AI solutions in Italy.

At EU level, the European Commission's High-Level Expert Group on Artificial Intelligence published the [Ethics Guidelines for Trustworthy AI in 2019](#). Although non-binding, those guidelines identify seven key requirements for trustworthy AI: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability. These principles have significantly influenced the human-centric and risk-based approach subsequently adopted by the AI Act.

Law stated - 16 September 2026

TAXATION

Online sales

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

Online sales are subject to regular taxation according to the principle of territoriality and the nationality of transferors and transferees. Treaties between some countries exist to avoid double taxation.

Law stated - 16 September 2026

Server placement

55 | 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?

In general, the principle of territoriality applies. This relates to the countries in which:

- a supplier's head office and a customer's head office are located or the countries in which their branch offices, if any, are located; or
- the countries in which they have identified themselves for tax purposes, regardless of the location of their servers.

The principle of territoriality is generally connected to the country in which the head office of a supplier and buyer are located. Local legislation cannot be excluded with regard to the location of servers in countries other than those in which the companies have their registered or secondary offices or where they are registered for tax purposes.

Law stated - 16 September 2026

Electronic invoicing

- 56** | 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?

The obligation of electronic invoicing was introduced by the [2018 Budget Law](#) (article 1, paragraphs 909, 916 and 917).

Initially, it was provided with reference only to gasoline and diesel supplies and services provided by subcontractors to the main contractor, in a contract with a public administration.

On 1 January 2019, the electronic invoicing requirement was extended to all supplies of goods and services between businesses and to final consumers.

From 1 July 2022, the electronic invoicing obligation is extended to taxpayers under the flat rate and advantage regime who received compensation exceeding €25,000 in 2021.

Electronic invoices are conveyed through the *Sistema di Interscambio* managed by the Internal Revenue Service, which keeps all invoice data.

Law stated - 16 September 2026

DISPUTE RESOLUTION

Venues

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

There are no specialist courts exclusively dedicated to online or digital disputes in Italy. Such disputes are generally heard by ordinary civil, criminal or administrative courts, depending on the subject matter, although specialised business divisions may have jurisdiction over certain matters such as intellectual property, unfair competition, antitrust or corporate disputes. EU digital regulations, including the GDPR, Digital Services Act, Digital Markets Act (DMA) and Data Act, are directly applicable in Italy and may be applied by Italian courts and, where relevant, by national independent authorities, without prejudice to the European Commission's central enforcement role under the DMA.

Law stated - 16 September 2026

ADR

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

There are several ADR methods provided by law:

- amicable settlements, mediation and judicial conciliation;
- arbitration as an alternative means of dispute resolution to a court decision, as provided for by section 806 of the Code of Civil Procedure; and
- sector-specific online conciliation procedures, including AGCOM's ConciliaWeb platform for disputes between users and providers of electronic communications services, including fixed and mobile telephony, internet and pay-TV services.

The Consumer Code provides a voluntary out-of-court settlement procedure for domestic and cross-border disputes between consumers and professionals residing and established in the EU. Under this procedure, an ADR body provides a solution for the parties or brings the parties together to facilitate an amicable settlement.

The DSA also applies in out-of-court dispute resolution mechanisms with regard to decisions of online platforms related to illegal content (article 21 of the DSA).

ADR methods are not widely used in Italy, but their use is increasing, particularly due to the digitalisation of procedures and the introduction of mandatory conciliation attempts in key regulated sectors, such as electronic communications and energy.

Law stated - 16 September 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

The new [Artificial Intelligence Act](#), which entered into force on 1 August 2024, is being implemented in phases, with full application expected by mid-2027 and may well increase productivity in the digital world, as well as improve innovation and digital processes. One foreseeable impact is that many companies are already adopting artificial intelligence to maintain a competitive edge in the digital marketplace.

The [Digital Services Act](#), which as of 17 February 2024, applies to all platforms, provides better protection for consumers and their rights online and establish a transparency and accountability framework for online providers. The Act, in fact, aims to foster innovation, growth and competitiveness within the single market. There are, for example, new procedures for removing illegal online content. Essentially, online intermediary services fall under the scope of the [Digital Services Act](#).

The [Digital Markets Act](#), which entered into force on 1 November 2022 and become applicable on 2 May 2023, bans a number of practices commonly used by large platforms that act as 'gatekeepers'. The Digital Markets Act, among other things: applies only to the major providers of the basic platform services most inclined to unfair practices, such as search engines, social networks or online brokerage services, that meet the objective

legislative criteria to be designated as access controllers; sets quantitative thresholds as a basis for identifying presumptive access controllers; it will also have the power to designate firms to serve as access controllers, following a market survey; prohibits several clearly unfair practices, such as preventing users from uninstalling preinstalled software or applications; and requires access controllers to proactively put in place certain measures, such as targeted measures that enable third-party software to function properly and interoperate with their services.

These trends are expected to affect online businesses and digital transformation projects by requiring stronger governance of digital advertising, environmental claims, influencer marketing and platform design, as well as greater investment in cybersecurity, ICT risk management and age-verification tools. At EU level, [the Digital Omnibus](#) proposals should also be monitored, as they may simplify or adjust certain compliance obligations under digital legislation, including data protection, cybersecurity, data access and AI rules. The proposed Digital Networks Act should also be monitored, as it is expected to reshape the EU regulatory framework for electronic communications networks and digital infrastructure, including Directive (EU) 2018/1972, although its final scope and timeline remain under discussion.

Law stated - 16 September 2026



Paolo Balboni
Luca Bolognini
Raffaella Cesareo
Luciana Di Vito
Camilla Serraiotto
Claudio Partesotti

paolo.balboni@ictlc.com
 luca.bolognini@ictlc.com
 raffaella.cesareo@ictlc.com
 luciana.divito@ictlc.com
 camilla.serraiotto@ictlc.com
 claudio.partesotti@ictlc.com

ICT Legal Consulting

[Read more from this firm on Lexology](#)

Serbia

[Jelena Hrle](#), [Dragoljub Sretenovic](#), [Tomislav Popović](#), [Bogdan Ivanišević](#),
[Anja Gligorević](#)
[BDK Advokati](#)

Summary

LEGAL AND REGULATORY FRAMEWORK

- Government approach
- Legislation
- Regulatory bodies
- Jurisdiction
- Establishing a business

CONTRACTING ON THE INTERNET

- Contract formation
- Applicable laws
- Electronic signatures
- Breach

FINANCIAL SERVICES

- Regulation
- Electronic money and digital assets
- Digital and crypto wallets
- Electronic payment systems
- Online identity

DOMAIN NAMES AND URLS

- Registration procedures
- IP ownership

ADVERTISING

- Regulation
- Targeted advertising and online behavioural advertising
- Misleading advertising
- Restrictions
- Direct email marketing

ONLINE PUBLISHING

- Hosting liability
- Content liability
- Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

As a small country and a non-EU member state, Serbia lags behind most other European jurisdictions in regulating digital content and services. In the matters of data protection, cybersecurity, and the use of artificial intelligence, national laws resembling those in the EU have been passed or are being drafted. Some other segments – including online publishing and copyright in the digital market – remain under-regulated. The laws passed so far related to digital content and services remain largely untested, with the partial exception of the law on the processing of personal data.

Law stated - 20 August 2026

Legislation

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

The most relevant laws governing digital content and services, digital transformation and the conduct of business online are the [Consumer Protection Act](#), the [Data Protection Act](#), and the [e-Commerce Act](#). Serbia has not taken steps yet to enact laws analogous to the Digital Services Act, Digital Markets Act, or Data Act.

Law stated - 20 August 2026

Regulatory bodies

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

The relevant regulatory bodies are the [Commissioner for Information of Public Importance and Personal Data Protection](#) (data protection) and the [Regulatory Authority for Electronic Communications and Postal Services](#) (RATEL) (telecommunications and cybersecurity).

Law stated - 20 August 2026

Jurisdiction

- 4 |

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?

There are no specific rules on the international jurisdiction of Serbian courts for online disputes. The Serbian system of international private law provides for a general jurisdiction of Serbian courts if the defendant has a seat or domicile in Serbian. In the absence of the seat or domicile of the defendant in Serbia, the Serbian court may also have jurisdiction (1) if the tortious act or damage has occurred in Serbia, (2) if the assets of the defendant or the claimed object is in Serbia (3) in case of consumer contract if the consumer resides in Serbia, (4) if the parties agreed to the jurisdiction of Serbian courts.

There are no rules on the exclusive international jurisdiction of Serbian courts in cases involving online transactions or in cases involving consumers.

Law stated - 20 August 2026

Establishing a business

5 | 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?

There are no separate regulatory and procedural requirements for the establishment of a digital business in Serbia.

An entity may operate a digital business in one of the four forms that also apply to offline businesses: (1) general partnership; (2) limited partnership; (3) limited liability company; or (4) joint stock company. Operators can choose from these four forms in which they would like to conduct business, the most common being limited liability companies.

Incorporation of entity for all four legal forms involves the following steps: (1) preparing the incorporation documents and registering with the commercial registry, (2) obtaining the qualified electronic signature for the legal representatives, (3) registering the ultimate beneficial owners, and (4) opening a bank account in Serbia.

Law stated - 20 August 2026

CONTRACTING ON THE INTERNET

Contract formation

6 | 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?

[Electronic Commerce Act](#) provides that a contract may be concluded using electronic means unless: (1) a special law prohibits e-signing, (2) the law requires the contract to be in the form of a solemnised document, a notarial record, or the signatures of the contracting

parties to be authenticated, or (3) in surety contracts the person granting surety acts outside of its trade, business or profession.

In contracts concluded using electronic means, offer and acceptance are exchanged through electronic communication. Such a contract is formed when the offeror receives the acceptance of the offer through electronic communication.

Law stated - 20 August 2026

Applicable laws

- 7 | 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?

Parties in business-to-consumer and business-to-business contracts concluded in an international setting may choose the applicable law. The choice of the governing law may be restricted only exceptionally by the application of overriding mandatory norms or public order. There are no special rules of Serbian private international law that limit the choice of governing law for contracts concluded by electronic means or for business-to-consumer contracts. Case law and legal doctrine in Serbia have not articulated a position on whether provisions of the [Consumer Protection Act](#) amount to overriding mandatory norms that would apply to contracts regardless of the chosen law, and whether in the case of consumer contracts, the choice of foreign law might be denied application on the ground of the public policy.

Contracts concluded by electronic means, including both business-to-consumer and business-to-business contracts, may be executed in a foreign language. However, in the case of business-to-consumer contracts, certain precontractual information must be provided in Serbian.

Contracting parties in contracts concluded by electronic means in an international setting may choose the forum for disputes without any restrictions.

Law stated - 20 August 2026

Electronic signatures

- 8 | 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?

The Electronic Document, Electronic Identification and Trust Services in Electronic Business Act ([Electronic Document Act](#)) provides for three types of e-signatures distinguished by the level of security they provide in legal transactions: (1) an electronic signature, (2) advanced electronic signature and (3) qualified electronic signature.

Qualified electronic signatures, a type of advanced electronic signatures, offer the maximum level of security as they are issued only by a qualified trust service which

is registered in the [Registry of Qualified Trust Service Providers](#) within the Ministry of Information and Telecommunications.

A qualified electronic signature holds the same legal validity as a handwritten signature. In situations where a handwritten signature is not mandatory, an electronic signature may be used. However, contracts and other legal documents for which a specific law provides that they must be made in the form of notarised signatures, publicly certified (solemnised) documents, or in the form of notarial deeds, cannot be made using electronic signatures.

Law stated - 20 August 2026

Breach

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

There are no special forums for the breach of contracts concluded online nor any online dispute resolution mechanism.

Law stated - 20 August 2026

FINANCIAL SERVICES

Regulation

- 10 | 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?

Relevant regulations protect consumers in the case of digital advertising or selling of financial services. The regulations provide, among other things, that:

- customers must receive comprehensive information from the service provider before a contract is concluded;
- customers may withdraw from the contract during a cooling-off period of 14 days, subject to certain exclusions;
- the service provider must not use abusive marketing practices seeking to oblige customers to buy a service they have not solicited; and
- the service provider must not use practices such as unsolicited phone calls and e-mails.

Law stated - 20 August 2026

Electronic money and digital assets

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

The [Payment Services Act](#) contains rules on, among other things, the issuance of electronic money, its distribution and redeemability, as well as authorisation and supervision of electronic money institutions. The law broadly follows the [EU E-Money Directive 2009/110/EC \(EMD2\)](#).

Serbia has separate legislation dedicated to cryptocurrencies and other instruments referred to as 'digital assets'. The [Digital Assets Act](#) applies to the issuance and admission to trading of digital assets in Serbia, the authorisation and supervision of digital assets service providers, anti-money laundering rules, and other matters related to digital assets.

Law stated - 20 August 2026

Digital and crypto wallets

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

The custody and administration of digital assets on behalf of third parties is a type of digital asset service that can only be carried out by licensed digital asset service providers (DASPs). The DASPs are subject to the initial capital requirements in the amount depending on the nature of the digital asset services provided. At least half of the initial capital must be contributed in money; the rest can be contributed in kind (eg, software).

The law imposes various other requirements on the DASPs, including organisational requirements, the rules on the safekeeping of clients' funds, the obligation to act honestly, fairly and professionally, etc.

Law stated - 20 August 2026

Electronic payment systems

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

The most recent amendments to the [Payment Services Act](#) have introduced open banking services to the Serbian market. The amendments regulate two new services: account information services and payment initiation services, in a manner that is meant to mirror the [EU Second Payment Services Directive](#).

Account information service is an online service that provides consolidated information on one or more payment accounts held by the payment service user (PSU) with one or more payment service providers.

A payment initiation service is a service to initiate a payment order at the request of the PSU with respect to a payment account held at another payment service provider. This includes businesses that enable PSU to purchase goods and services online without using a payment card or another payment method.

Law stated - 20 August 2026

Online identity

- 14** | 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 [AML Act](#) generally requires all obliged entities, including financial institutions and DASPs, to take customer due diligence measures when onboarding new customers, that is, establishing a business relationship.

The customer due diligence measures generally include customer identification and verification, beneficial ownership identification and verification, understanding the nature and purpose of customer relationships, ongoing monitoring for reporting suspicious transactions, and maintaining and updating customer information.

As a rule, the customer must be physically present for identification. Exceptionally, the verification of the customer's certificate can be conducted by using: (a) video technology; or (b) the qualified electronic certificate, in both cases without the customer's physical presence. The regulations of the [National Bank of Serbia](#) (NBS) set out the conditions for the use of video technology to identify and verify the identity of the customers of financial institutions and DASPs, who are natural persons or entrepreneurs, or natural persons who are legal representatives of the customers, which are legal entities.

Law stated - 20 August 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15** | 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 Serbian National Internet Domain Registry Foundation (RNIDS) manages the registration of national internet domain names .rs and .cpb through accredited registrars. RNIDS established procedures for the registration of national domain names in the [General Terms and Conditions for the Registration of National Internet Domains](#) and the [Procedure for the Registration of National Internet Domains](#).

Both national and foreign individuals or entities may register a national domain name. The procedure involves submitting a registration request to an accredited registrar, paying applicable fees, and activating the domain name. There are no restrictions on the use of URLs to direct users to particular websites, online resources or metaverse.

Law stated - 20 August 2026

IP ownership

- 16** | 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?

A domain name may be registered as a trademark or protected by copyright if it meets the specific requirements for trademark or copyright protection.

Under certain conditions, ownership of a copyright or trademark may be useful in challenging a competitive use or registration of a similar domain name. According to the General Terms and Conditions for the Registration of National Internet Domain Names, a domain name must not infringe on IP rights or other rights of a third party. The right holder can initiate alternative dispute resolution for an infringing domain name before the Commission for Resolution of Disputes Regarding the Registration of National Internet Domains at the Chamber of Commerce of Serbia and request the transfer or cancellation of the infringing domain name. Depending on the specific circumstances, the copyright or trademark holder may be able to file a lawsuit in a competent court for infringement of IP rights.

Law stated - 20 August 2026

ADVERTISING

Regulation

- 17** | What rules govern online advertising?

The [Advertising Act](#) is the principal legal instrument directly governing online advertising. The Act uses the term 'Internet advertising' for advertising through online editions of traditional media (press, radio, television) and registered Internet portals, social networks, applications, or through another form of Internet communication. Other laws impact online advertising by regulating profiling ([Data Protection Act](#)), the use of cookies ([Electronic Communications Act](#)), and misleading commercial practices ([Consumer Protection Act](#)).

Law stated - 20 August 2026

Targeted advertising and online behavioural advertising

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

As targeted advertising and online behavioural advertising are predicated upon the creation of a 'profile' of the targeted individual, the relevant rules are those on profiling and use of cookies, from the Data Protection Act and the Electronic Communications Act respectively. The [Data Protection Act](#) grants the data subject a right to object to the processing of personal data concerning him or her which is based on profiling based on the

legitimate interests of the data controller or a third party. The [Electronic Communications Act](#) states that storing cookies on the end user's terminal equipment requires the end user's prior consent.

Law stated - 20 August 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

There are no specific rules on misleading online advertising. The general rule from the Advertising Act applies, to the effect that advertising is prohibited if it deceives or is likely to deceive the recipients of the advertising message and, by reason of its deceptive nature, it may affect their economic behaviour, or for those reasons injures or is likely to injure a competitor. The prohibition of misleading advertising applies irrespective of the industry.

Additionally, the Consumer Protection Act prohibits misleading commercial practices, offline and online, including some specific forms of advertising.

Law stated - 20 August 2026

Restrictions

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

The grounds for the prohibitions of online advertisements are the same as the general grounds for prohibition under the Advertising Act. As a result, advertisement of pornography, narcotic drugs, weapons, military equipment, tobacco and tobacco products is prohibited, as is advertisement of games of chance directed at minors and advertisement of most types of alcoholic beverages. The [Medicines and Medical Devices Act](#) prohibits various modes of advertising of medicines, including the advertising of prescription drugs and medicines issued at the expense of health insurance funds.

Law stated - 20 August 2026

Direct email marketing

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

The Data Protection Act allows direct marketing unless the data subject objects to processing for direct marketing purposes. However, a series of other laws – Consumer Protection Act, [e-Commerce Act](#), Advertising Act, and the Electronic Communications Act – prohibit direct marketing via devices for distant communication, including but not limited to telephone, fax machine or email, unless the individual has given his or her prior consent.

Law stated - 20 August 2026

ONLINE PUBLISHING

Hosting liability

- 22** | 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?

Parties that merely host the content written or published by third parties might have intermediary liability if they fail to remove any information whose unlawful nature was known, or should have been known, to the hosting provider. No law requires the hosting provider to proactively monitor to identify unlawful content. Under the [e-Commerce Act](#), service providers are not liable for the information stored at the request of a recipient of the service, on condition that: (1) the provider did not have and could not have had knowledge of the illegal activity of the recipient of the service or the content of the information; or (2) the provider, upon obtaining such knowledge, acts expeditiously to remove or to disable access to the information.

Law stated - 20 August 2026

Content liability

- 23** | 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?

Where a digital platform or online content provider itself publishes the information, the rules on the liability for unlawful content do not differ from those for the publication of content in traditional settings, that is, print and electronic media. It is possible to avoid liability if the platform or online content provider may justify in the specific instance the publication of the information on the grounds of freedom of speech.

Law stated - 20 August 2026

Shutdown and takedown

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

An internet service provider or telecommunications provider can shut down a web page containing defamatory material, without court authorisation.

Law stated - 20 August 2026

INTELLECTUAL PROPERTY

Data and databases

25 | Are data and databases protected by IP rights?

Data may be protected as trade secrets if they meet the following conditions: the data are secret in the sense that they are not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; the data have commercial value due to the secrecy; and, the data have been subject to reasonable steps to keep them secret.

Databases enjoy copyright protection if the selection or arrangement of their contents is original and meets other requirements for copyright protection. The contents themselves are not within the scope of copyright protection. Databases that are not eligible for copyright protection may be subject to database rights, a category of related rights providing the right holder exclusive control over extraction and re-utilisation of all or substantial parts of the database's contents for a 15-year period.

Law stated - 20 August 2026

Third-party links and content

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

The issue of linking to third-party copyrighted content has not been addressed in case law. Serbian courts would likely seek guidance from the rulings of the Court of Justice of the European Union on the issue, from which it follows that linking to publicly available copyrighted works is generally allowed, if the linking does not bypass any access restrictions, such as a paywall.

Law stated - 20 August 2026

27 | 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?

Using third-party copyrighted content, including material obtained through automated scraping, without the copyright holder's permission, risks copyright infringement. The use of copyrighted works without permission is only allowed in specific cases defined by law as exceptions or limitations. Examples of permitted uses include quotation, use of a work as an insignificant part of another work, adaptation of a work for the purpose of parody or caricature, or reproduction of extracts of a work for the purpose of scientific research. The copyright law still does not contain the text and data mining exceptions analogous to those under [Copyright Directive 2019/790/EU](#) (articles 3 and 4).

If the online content provider intends to use the contents of a publicly available database protected by database rights, such use is arguably lawful unless the maker of the database

is able to prove damage. The use is not lawful if the user of the website explicitly accepts the terms of use that prohibit the use of the webpage data.

Law stated - 20 August 2026

Metaverse and online platforms

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

The challenges related to establishing and defending IP rights in metaverse may arise, for example, from the difficulties in identifying infringers and determining the appropriate jurisdiction.

Law stated - 20 August 2026

Exhaustion of rights and first-sale doctrine

- 29** | 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?

Serbian law recognises the concept of exhaustion of rights in relation to all IP rights, with certain variations. Under copyright law, once the author or their legal successor places a copy of a work on the Serbian market, their exclusive rights to distribute that copy are exhausted. The law does not address the exhaustion of rights in digital products, and no case law has been established on the matter. It is likely that Serbian courts would look for guidance in the relevant rulings of the Court of Justice of the European Union. Under the Court's case law, reselling lawfully downloaded software is permitted if the original transaction can be considered a genuine sale ([UsedSoft case, C-128/11](#)), while providing e-books constitutes a communication to the public (and not sale) and therefore does not result in exhaustion of rights ([Tom Kabinet case, C-263/18](#)).

Law stated - 20 August 2026

Administrative enforcement

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

Inspection authorities may conduct dawn raids in connection with IP infringement, but they are not authorised to issue freezing injunctions. Inspection authorities may impose various actions, such as preventive measures and corrective measures to remedy any identified non-compliance. In case of a punishable infringement, the inspection authority may initiate criminal, misdemeanour, or commercial offence proceedings. Where the law

specifies only a fixed monetary fine for a misdemeanour, inspection authorities can issue a misdemeanour order, imposing the sanction directly without initiating court proceedings.

Law stated - 20 August 2026

Civil remedies

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

Civil remedies (including provisional measures) available to IP owners include, among others:

- determination of infringement or serious threat of infringement;
- prohibition of acts of infringement or serious threat of infringement;
- compensation for material and non-material damages;
- seizure, removal from the market, or destruction of infringing goods;
- publication of the judgement;
- freezing injunctions, specifically seizure of assets and prohibition of making payments; and
- dawn raids, to preserve evidence by taking a detailed description of infringing objects, collecting samples, seizing the objects and the means used for their creation and distribution, and any related documents.

Law stated - 20 August 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

32 | 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 [Data Protection Act](#) defines 'personal data' as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified directly or indirectly, particularly through identifiers like a name, ID number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

Special categories of personal data include information revealing racial or ethnic origin, political opinions, religious beliefs, union membership, health data, genetic data, biometric data for identification, and data concerning sexual orientation. Processing such data is generally prohibited unless one or more of the ten conditions prescribed by the Act are met.

Pseudonymous data refers to data processed in a way that it cannot be attributed to a specific person without additional information. Pseudonymisation does not remove the data from the law's protections.

Although the Act does not explicitly define anonymous data, it implies that anonymised data, which cannot be traced back to an individual, falls outside the scope of personal data protection.

Law stated - 20 August 2026

Registration and appointment of data protection officer

- 33** | 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?

Parties involved in processing personal data are not required to register with a regulator to carry out data processing.

The Data Protection Act mandates the appointment of a Data Protection Officer (DPO) in specific cases, similar to the General Data Protection Regulation (GDPR). A DPO must be appointed when processing is conducted by a public authority or body (excluding courts in their judicial role), or when the core activities of the controller or processor involve large-scale, regular and systematic monitoring of individuals or the processing of special category data or data relating to criminal convictions.

Law stated - 20 August 2026

Extraterritorial issues

- 34** | 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 Data Protection Act applies to organisations or individuals outside Serbia if they offer goods or services to individuals within Serbia, regardless of whether payment is required, or if they monitor the behaviour of individuals in Serbia. Such organisation or individual is, with some exceptions, required to appoint a representative in Serbia. The representative acts as a point of contact for data subjects, the Serbian data protection authority, and third parties.

Law stated - 20 August 2026

Bases for processing

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

The Data Protection Act provides several grounds for lawful data processing. These include the consent of the data subject, often relied upon when no other legal basis is applicable and generally used in the context of marketing activities. Processing is also lawful when it is necessary for the performance of a contract, such as fulfilling customer orders, or for compliance with legal obligations, like employment laws.

Another legal basis is a legitimate interest, which allows organisations to process data if their interests don't override the rights of the data subject. This is common in fraud detection, network security, and certain employment-related processing. Additionally, vital interests justify processing when necessary to protect someone's life or health, while public interest or official authority can also serve as a legal ground for processing.

International transfers must additionally meet specific requirements, like adequacy decisions, standard contractual clauses, or binding corporate rules to protect data when they leave Serbia.

Law stated - 20 August 2026

Data export and data sovereignty

- 36** | 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?

Transfers to countries recognised by the EU as providing an adequate level of protection or to signatories of the Council of Europe's Convention 108 can occur without additional requirements.

For transfers to other countries, Serbian law outlines several safeguards. Most frequently used in practice are standard contractual clauses issued by the Serbian Data Protection Commissioner. Those clauses apply only to controller-to-processor transfers.

In certain circumstances, transfers can take place based on data subject's explicit consent, or because transfers are necessary for contract performance, public interest, legal claims, or the protection of vital interests.

Serbian law does not impose any requirements that data or servers must remain within the country.

Law stated - 20 August 2026

Sale of data to third parties

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

The general rules of data processing apply to transfers of personal data to third parties, including the requirement for a valid legal basis (eg, consent or legitimate interest) or the

obligation to notify the data subject. If the recipient is located in a third country, the rules on international transfers must also be followed.

The seller is responsible for ensuring the lawful processing of personal data before the transfer and for the legality of the transfer itself. If the recipient is a controller, it assumes full responsibility for ensuring that the data is subsequently processed in compliance with the law. If the recipient is a processor, they act on behalf of the controller and must process the data only according to the controller's instructions. The controller must ensure that there is a clear data processing agreement in place, outlining the processor's obligations and safeguards.

Law stated - 20 August 2026

Consumer redress

38 | 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?

Under the Data Protection Act, individuals—regardless of nationality or residency—have several rights and remedies concerning the processing of their personal data. They have the right to access, correct, delete, and restrict the processing of their data, as well as to request data portability where applicable. Additionally, they can object to processing for direct marketing or any processing based on legitimate or public interest, including profiling. Individuals are also protected from decisions made solely through automated processing if those decisions have significant effects on them.

For remedies, individuals can file complaints with the data protection authority or seek judicial redress, including compensation for damages resulting from unlawful data processing. These rights apply to anyone whose data is processed under Serbian law.

Law stated - 20 August 2026

Non-personal data

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

Various sector-specific laws indirectly impact the usage, storage, and sharing of non-personal data. Some examples are the [Free Access to Information of Public Importance Act](#), which regulates the right of the public to access information held by public authorities, or the [Protection of Trade Secrets Act](#), which restricts unauthorised access and usage of confidential business information classified as trade secrets, safeguarding data that holds commercial value.

Law stated - 20 August 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

- 40** | 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 [Electronic Document, Electronic Identification and Trust Services in Electronic Traffic Act](#), any document may be kept exclusively in electronic format, provided that the electronic document is an original (ie, created initially in digital format) or that an electronic copy of the original paper document is considered equivalent to the original.

Law stated - 20 August 2026

Retention

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

Various pieces of legislation prescribe minimum retention periods for documents or data. For example, records in the areas of employment, healthcare, and accounting must be kept permanently or for a specified number of years. Only the [Data Protection Act](#) establishes a maximum retention period for personal data: pursuant to the 'storage limitation' principle, personal data may only be retained for as long as necessary to fulfil the purpose of data processing.

Law stated - 20 August 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

Companies are obliged to implement technical, organisational and personal measures to ensure the security of the processing of personal data in accordance with the [Data Protection Act](#). These measures may include pseudonymisation and encryption, maintaining confidentiality, integrity, availability and resilience of systems and services, and ensuring rapid data availability after incidents. Regular testing and evaluation of the effectiveness of security measures are also required. Additionally, individuals authorised to access personal data must process it only under the controller's instructions or legal obligations. The newly adopted [Information Security Act](#) requires operators of information and communication systems of special importance, classified as "priority" or "important" systems, to adopt a comprehensive set of measures to prevent security incidents and mitigate any resulting damage.

Law stated - 20 August 2026

Data breach notification

- 43** | 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?

The Data Protection Act, the Information Security Act, and the [Electronic Communications Act](#) apply to digital (and non-digital businesses) and contain provisions on data breach notifications.

Pursuant to the Data Protection Act, if a personal data breach poses a risk to individuals' rights and freedoms, the data controller must inform the Data Protection Commissioner. Additionally, if the breach presents a high risk to individuals' rights and freedoms, the controller must as a rule notify the affected individuals.

The Information Security Act mandates that operators of ICT systems of special importance report incidents that could significantly compromise information security. This law does not require notifying individuals.

Under the Electronic Communications Act, when there is a significant security and integrity breach impacting public electronic communications networks and services, the entity involved must notify the Regulatory Authority for Electronic Communications and Postal Services (RATEL).

Law stated - 20 August 2026

Government interception

- 44** | 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?

The main entities empowered to request data are the intelligence agencies, including the Security Information Agency (BIA), the Military Intelligence Agency, and the Military Security Agency, alongside law enforcement authorities such as public prosecutors. These agencies are tasked with national security, defence, and criminal investigations, and are authorised under laws such as the [Security Information Agency Act](#), the [Military Security and Military Intelligence Agency Act](#), and the [Criminal Procedure Code](#). Intelligence agencies may request data from any person or organisation, covering broad sectors without limitations, although data collection from individuals by the Military Security Agency is subject to their consent. Public prosecutors may also demand data from any third parties for criminal investigations.

The scope of data collection is generally broad, allowing agencies to request any information relevant to national security or the prosecution of criminal activities. Intelligence agencies can seek data to protect Serbia's security and defence interests, while public prosecutors can request data essential to gathering evidence in criminal cases. Public

prosecutors need court approval for telecommunications surveillance or property raids but not for general data requests or item seizures.

Law stated - 20 August 2026

GAMING

Legality and regulation

- 45** | 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?

Online gaming business is permitted, provided that the entity obtains a licence for organising games of chance from the Serbian gaming authority. This licence may be granted to companies established in Serbia that meet specific regulatory requirements, including criteria related to share capital, financial standing, and technical conditions.

The licence can cover online betting or any digital game based on a random number generator. However, only the state-owned lottery company may organise online lottery games.

Individuals under 18 years of age cannot register and play on online gaming platforms.

Law stated - 20 August 2026

Cross-border gaming

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

Online gaming businesses not licensed in Serbia are prohibited from offering gaming products on a cross-border basis, as Serbian law restricts unlicensed entities from organising games of chance. Furthermore, the legislation prohibits participation in games of chance organised abroad if stakes are paid within Serbia. In practice, this means that foreign online gaming operators cannot offer their gaming products to players in Serbia. This restriction also applies to advertising, which is only permitted for entities licensed under Serbian regulations.

Law stated - 20 August 2026

OUTSOURCING

Key legal issues

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

Outsourcing is not regulated by Serbian law, however, staff leasing is, and it is a licensed business activity. The [Staff Leasing Act](#) prescribes a so-called staff leasing presumption, according to which a person working for or at the premises of a beneficiary while being employed or engaged outside employment by another employer, is presumed to be a leased employee unless proven otherwise. Therefore, when outsourcing services in Serbia, both the service provider and the client must ensure that their arrangement cannot be mistaken for staff leasing.

The law does not prescribe criteria for establishing staff leasing and there is no enforcement practice yet. However, it is reasonable to assume, and the Ministry of Labour confirmed so unofficially at various seminars, the beneficiary's control over the employee's work is a factor indicating staff leasing. Employee's presence on the beneficiary's premises and use of the beneficiary's means of work can also indicate staff leasing.

The risk that the Ministry of Labour or courts would consider outsourcing outside Serbia as staff leasing does not apply.

Law stated - 20 August 2026

Sector-specific issues

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

The National Bank of Serbia (NBS) has enacted specific regulations covering the outsourcing arrangements entered into by a financial institution (FI) and in particular the outsourcing of the activities relating to the FI's information systems. The FI is required to notify the NBS before entering into an outsourcing agreement. In case of outsourcing to a service provider abroad, the FI would also need to provide evidence that the regulations of the host country of such service provider allow the NBS to exercise its supervisory functions in relation to or in connection with the outsourced activities.

The FI is obliged to deliver to the NBS the executed outsourcing agreement and any annexes thereto (which do not affect the scope of the outsourced activities, the service provider, or the FI's risk analyses) within 15 days, as well as to notify the NBS about termination of the outsourcing agreement.

Law stated - 20 August 2026

Contractual terms

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

No.

Law stated - 20 August 2026

Employee rights

- 50** | 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?

The law does not provide special protection for outsourced employees in the event of a business transfer (eg, the right to consultations or the right to maintain the same level of rights, including compensation). Such protection is guaranteed only in cases of status changes (eg, mergers or spin-offs) or other instances of universal legal succession.

Law stated - 20 August 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

AI is not yet regulated in Serbia. Automated decision-making, including profiling, is regulated under the [Data Protection Act](#), with provisions mirroring those in the General Data Protection Regulation (GDPR). Individuals have the right not to be subject to decisions based solely on automated processing (including profiling) that have legal or similarly significant impacts, unless specific conditions are met, such as the individual's explicit consent. It is advisable to conduct a data protection impact assessment when processing personal data in the context of developing or using AI, machine learning, or automated decision-making and profiling.

Law stated - 20 August 2026

IP rights

- 52** | 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?

Serbian law does not specifically address IP rights in the context of AI and machine learning. There are no legal obstacles to protecting training datasets by IP rights, if the requisite conditions are met, such as originality in the case of copyright protection. As a general rule, AI-produced outputs are not eligible for copyright protection because the [Copyright Act](#) grants copyright protection only to works created by humans as authors.

Law stated - 20 August 2026

Ethics

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

The Serbian Government has adopted [Ethical Guidelines for the Development, Application and Use of Reliable and Responsible Artificial Intelligence](#). The Guidelines outline four principles of ethical AI (explainability and verifiability, dignity, prohibition of causing damage, and fairness), as well as preconditions for reliable and responsible AI (such as transparency, diversity, non-discrimination and equality). The Guidelines provide a non-exhaustive list of high-risk AI systems, including those employed in the fields of healthcare, employment, and law enforcement.

Law stated - 20 August 2026

TAXATION

Online sales

- 54** | Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Income from the sale of digital products and online services is subject to the corporate income tax in the same manner as any other income. Resident entities (ie, the ones that are established or have a place of effective management and control in Serbia) are subject to the corporate income tax on their net income from any country. Non-resident entities are taxed on the net income only if they have created a permanent establishment in Serbia and only to the extent that income can be attributed to such a permanent establishment.

When a resident entity sells its digital assets at a gain, such gain is in principle taxable (except in the case of licensed entities dealing in digital assets). The gain may be exempt from the corporate income tax if the entity reinvests the proceeds into the equity of a resident company or in an investment fund having its centre of investment activity in the country.

The value added tax (VAT) is levied at the standard rate of 20 per cent on supplies of goods and services that are deemed to have their place in Serbia. The sale of digital products and the provision of online services are considered as a taxable supply of services for the purposes of VAT. A specific exemption from VAT exists for financial services of transfer of virtual currencies and their exchange for money.

A foreign entity that supplies taxable or exempt services deemed to have their place of supply in Serbia exclusively to business customers does not have to register as a Serbian VAT payer. The entity must register as a Serbian VAT payer if it supplies a service deemed to have its place of supply in Serbia to non-business customers. This is done by appointing a local VAT representative, who is a resident VAT payer and must be preapproved by the

Serbian tax authority. Once approved, the local VAT representative performs all obligations of a taxpayer in the name and on behalf of the foreign entity, including issuance of invoices to customers, keeping VAT records, filing VAT returns, paying VAT, and other.

Law stated - 20 August 2026

Server placement

- 55** | 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?

Placing a server as a piece of hardware on the Serbian territory could theoretically lead to the creation of a fixed place through which a business is fully or partially carried on, and therefore to the creation of a permanent establishment of a foreign entity that operates such server. This would be possible provided that the foreign entity is the owner of the server or leases it, and that the server is used to carry out business activity (excluding activities of a preparatory or auxiliary nature, such as marketing, gathering market data, etc). However, this is only a theoretical possibility, not supported by any example from the case law or publicly available practice.

The mere presence of a platform or metaverse on a server located in Serbia could not be regarded as a fixed place through which a business is at least partially carried on, and therefore could not lead to the creation of a permanent establishment.

Law stated - 20 August 2026

Electronic invoicing

- 56** | 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?

Under the [Electronic Invoicing Act](#), all VAT payers, local VAT agents of foreign entities, and public sector entities are required to issue e-invoices and upload them on the Electronic Invoicing System. The tax authority has access to the System, and there is no requirement for the taxpayers to provide copies of e-invoices to the tax authorities.

Law stated - 20 August 2026

DISPUTE RESOLUTION

Venues

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

There are no specialist courts or other venues dealing with online/digital issues and disputes.

Law stated - 20 August 2026

ADR

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

ADR methods, such as arbitration and mediation, are generally available for disputes where parties can freely dispose of their rights, except in cases where the law prescribes exclusive jurisdiction of courts. While arbitration is available only in pecuniary disputes, mediation is available for all sorts of disputes, except those regarding public revenues.

ADR in Serbia is generally not commonly used.

There is a specific ADR means for the resolution of second-level domain disputes under the top-level domains .rs and .cpb organised by the [Committee for the resolution of disputes relating to the registration of national internet domain names](#) under the auspices of the Chamber of Commerce and Industry of Serbia. The dispute is resolved by a sole expert, unless one of the parties requests that the dispute is resolved by a three-member panel of experts. A sole expert is appointed jointly by the parties or, in the event of failure, by the Presidency of the Committee (all from, the List of Experts maintained by the Committee). In case of a three-member panel of experts, the parties appoint one expert each, and the appointed experts jointly choose the presiding expert (all from the List of Experts). Parties retain the right to seek judicial remedies.

In the area of consumer protection, there is the procedure for out-of-court resolution of consumer disputes before 'bodies for out-of-court resolution of consumer disputes'. The 'bodies' are individuals who qualify as mediators under the Mediation in the Resolution of Disputes Act and fulfil some additional qualifications. The bodies can issue recommendations, that are not binding, or terminate the proceedings if they are not meaningful, or the parties can reach a settlement. Parties retain the right to seek judicial remedies.

Law stated - 20 August 2026

UPDATE AND TRENDS

Key trends and developments

59 | 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?

In October 2025, the parliament adopted a new [Information Security Act](#), in response to [NIS2 Directive](#). In April 2026, a [new law on consumer protection](#) was also enacted, taking over a number of provisions from three EU directives adopted in 2019: [Directive \(EU\) 2019/770](#) on certain aspects concerning contracts for the supply of digital content and digital services; [Directive 2019/771/EU](#) on certain aspects concerning contracts for the sale of goods; and Enforcement and Modernisation Directive ([Directive \(EU\) 2019/2161](#)). Also, during 2026, a law was being drafted that, according to the government, would largely align with EU AI Act but would be less focused on placing limitations on the use of AI.

Law stated - 20 August 2026



Jelena Hrle
Dragoljub Sretenovic
Tomislav Popović
Bogdan Ivanišević
Anja Gligorević

Jelena.Hrle@bdkadvokati.com
dragoljub.sretenovic@bdkadvokati.com
Tomislav.Popovic@bdkadvokati.com
bogdan.ivanisevic@bdkadvokati.com
Anja.Gligorevic@bdkadvokati.com

BDK Advokati

[Read more from this firm on Lexology](#)

USA

Ieuan Jolly

Linklaters LLP

Summary

LEGAL AND REGULATORY FRAMEWORK

Government approach
Legislation
Regulatory bodies
Jurisdiction
Establishing a business

CONTRACTING ON THE INTERNET

Contract formation
Applicable laws
Electronic signatures
Breach

FINANCIAL SERVICES

Regulation
Electronic money and digital assets
Digital and crypto wallets
Electronic payment systems
Online identity

DOMAIN NAMES AND URLS

Registration procedures
IP ownership

ADVERTISING

Regulation
Targeted advertising and online behavioural advertising
Misleading advertising
Restrictions
Direct email marketing

ONLINE PUBLISHING

Hosting liability
Content liability
Shutdown and takedown

INTELLECTUAL PROPERTY

- Data and databases
- Third-party links and content
- Metaverse and online platforms
- Exhaustion of rights and first-sale doctrine
- Administrative enforcement
- Civil remedies

DATA PROTECTION AND PRIVACY

- Definition of 'personal data'
- Registration and appointment of data protection officer
- Extraterritorial issues
- Bases for processing
- Data export and data sovereignty
- Sale of data to third parties
- Consumer redress
- Non-personal data

DOCUMENT DIGITISATION AND RETENTION

- Digitisation
- Retention

DATA BREACH AND CYBERSECURITY

- Security measures
- Data breach notification
- Government interception

GAMING

- Legality and regulation
- Cross-border gaming

OUTSOURCING

- Key legal issues
- Sector-specific issues
- Contractual terms
- Employee rights

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

- Rules and restrictions
- IP rights
- Ethics

TAXATION

- Online sales
- Server placement
- Electronic invoicing

DISPUTE RESOLUTION

Venues

ADR

UPDATE AND TRENDS

Key trends and developments

LEGAL AND REGULATORY FRAMEWORK

Government approach

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

The United States' federalist system – with both a centralised federal government and regional state and local governments – can generate a diversity of legal and regulatory attitudes and approaches. Although, as a general matter, the governmental attitude and approach with respect to digital content and services, digital transformation and doing business online has been to seek to ensure that the US occupies a leadership position in the digital realm, including with respect to innovation, while mitigating risks and potential harms associated with digital and emerging technologies, the current presidential administration has been deprioritising risks and potential harms and instead focusing on leadership and innovation. One notable area in which the US government has recently sought to shift such balance is artificial intelligence (AI), as demonstrated by multiple executive orders on AI issued during President Trump's second term, starting with an executive order on 'Removing Barriers to American Leadership in Artificial Intelligence' (Trump Initial AI Policy Framework Executive Order) issued in the first week of his second term, which revoked the prior presidential administration's executive order on 'Safe, Secure, and Trustworthy Artificial Intelligence' (Biden AI Executive Order).

Law stated - 31 July 2026

Legislation

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

The US legislative and regulatory framework with respect to digital content and services is a complex matrix of both federal (national) and state laws, rules and regulations, both general and activity or sector-specific, covering a wide variety of legal areas and enforced by a variety of regulatory authorities and agencies.

Federal

The Federal Trade Commission Act (15 U.S.C. § 41 et seq) (FTC Act) is a federal consumer protection law that prohibits both (1) unfair or deceptive commercial acts or practices – which prohibition the Federal Trade Commission (FTC) has applied to such areas as consumer privacy, data security and false advertising – and (2) unfair methods of competition – which prohibition the FTC has used to enforce federal civil antitrust law.

Apart from such general laws as the FTC Act, there are myriad activity or sector-specific federal laws, rules and regulations that govern digital (as well as, under many of such laws, non-digital) content and services, including the following.

- Content:

- Title II [Online Copyright Infringement Liability Limitation] of the Digital Millennium Copyright Act (Public Law 105-304) (DMCA) added a new section to the federal Copyright Act (17 U.S.C. § 101 et seq) (Copyright Act) to create a series of limitations on liability for copyright infringement by online service providers.
- Title V [the Communications Decency Act] of the Telecommunications Act of 1996 (Public Law 104-104) (Telecommunications Act): (1) prohibits the transmission of obscene content via the internet and other telecommunications and provides civil or criminal penalties for violations; and (2) through its 'Good Samaritan' protection provision, excludes both providers and users of 'interactive computer services' from liability based on third-party content. With respect to the transmissions prohibited under clause (1) above, the Federal Communications Commission (FCC) has civil enforcement authority, while the US Department of Justice has criminal enforcement authority.
- E-commerce: Title III [the Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act] (INFORM Consumers Act) of Division BB [Consumer Protection and Commerce] of the Consolidated Appropriations Act 2023 (Public Law 117-328) imposes new obligations on 'online marketplaces' in which third parties sell 'consumer products' (which, based on the definition in the statute, is understood to mean only physical goods, and not digital products or intangible services), in order both to provide additional transparency for consumers and to stymie efforts of criminal actors to sell stolen, counterfeit or unsafe items through such online markets. Both the FTC and state attorneys general have authority to enforce the INFORM Consumers Act.
- Advertising and marketing:
 - The Controlling the Assault of Non-Solicited Pornography and Marketing Act (15 U.S.C. § 7701 et seq) (CAN-SPAM Act) governs 'commercial electronic mail messages', including emails and certain text messages. The FTC and state attorneys general have regulatory enforcement authority.
 - Both the Telephone Consumer Protection Act (47 U.S.C. § 227) (TCPA) and the Telemarketing Sales Rule (TSR) promulgated by the FTC under the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. § 6101 et seq) regulate, among other telemarketing activities, text message advertising and marketing. The FCC has regulatory authority under the TCPA, while the FTC has regulatory authority with respect to the Telemarketing and Consumer Fraud and Abuse Prevention Act, including enforcement authority with respect to the TSR.
- Data protection (including privacy and security):
 - The Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq) (GLBA), together with the rules and regulations promulgated thereunder (including the FTC's 'Standards for Safeguarding Customer Information' rule (16 C.F.R. § 314.4) (Safeguards Rule)), regulates the collection, use, protection and disclosure of non-public personal information by a range of institutions that engage in

financial activities. The GLBA is enforced by a myriad of regulators, including the FTC as well as, depending on the underlying industry and company, the Consumer Financial Protection Bureau (CFPB), the Commodity Futures Trading Commission (CFTC), and state insurance authorities.

- The Health Insurance Portability and Accountability Act (Public Law 104-191) (HIPAA), together with the Privacy Rule, Security Rule, Breach Notification Rule and Health Breach Notification Rule thereunder, governs individually identifiable health information collected or created as a consequence of the provision of health care by a 'covered entity'. The Department of Health and Human Services (HHS), acting through its Office for Civil Rights, is responsible for enforcing HIPAA.
- The Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq) (COPPA) imposes obligations on operators of websites, mobile apps, or other online services that are directed to children under 13 years of age, and on operators of other online services that have actual knowledge that they are collecting personal information from such children. The FTC is the primary enforcement authority with respect to COPPA, but state attorneys general and certain other federal agencies also have authority under the statute to enforce compliance within the specific industries they regulate.
- The Video Privacy Protection Act (18 U.S.C. § 2710) (VPPA) governs the disclosure and destruction of 'personally identifiable information' by 'video tape service providers', the definition of which includes not only 'prerecorded video cassette tapes', but also 'similar audio visual materials'. That broad definition has led to a wave of recent VPPA class action litigation related to the use of third-party technology (eg, pixels) on websites and other digital properties that play videos, under the VPPA's private right of action.
- The Red Flags Rule promulgated by the FTC and several other federal agencies under the Fair and Accurate Credit Transactions Act (Public Law 108-159), amending the Fair Credit Reporting Act (15 U.S.C. § 1681) (FCRA), imposes obligations on 'financial institutions' and 'creditors' to establish a written identity theft prevention programme that is designed to detect, prevent and mitigate identity theft in connection with 'covered accounts' and sets forth guidelines to assist with the formulation and maintenance of such a programme. The FTC and various financial, banking and other federal agencies have rulemaking and enforcement responsibility for the Red Flags Rule.
- Civil rights: The Americans with Disabilities Act (42 U.S.C. § 12101 et seq) (ADA) prohibits discrimination based on disability, and its provisions apply not only to digital content and services, but also to the accessibility of websites and digital properties. The US Department of Justice, which is the rulemaking and enforcement authority for the ADA, has issued guidance on web accessibility and the ADA.

State

US state consumer protection laws, like the FTC Act (on which many of such laws are modelled), typically include provisions applicable to digital content and services. In

addition, currently 23 US states have enacted general privacy laws that – given their broad definitions of ‘personal information’ and ‘personal data’ that include online identifiers such as cookie IDs and internet protocol addresses – impose significant obligations with respect to digital content and services. As of the end of July 2026, 19 of such state general privacy laws were in effect. State attorneys general are responsible for enforcing consumer protection laws and state general privacy laws, although, with respect to the California Consumer Privacy Act (CA Civ. Code § 1798.100 et seq) (CCPA), the California Privacy Protection Agency (CalPrivacy) also has implementation and enforcement authority. In addition, various agencies may have enforcement authority with respect to activity and sector-specific state laws, rules and regulations.

Law stated - 31 July 2026

Regulatory bodies

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

Answer in progress.

Law stated - 31 July 2026

Jurisdiction

- 4 | 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?

The rules and standards for establishing jurisdiction for online transactions or disputes are still evolving, with apparent splits among federal circuits and even reevaluation by the same circuit, as highlighted by a 2025 Ninth Circuit decision.

In *Briskin v Shopify, Inc.*, 108 F.4th 1003, WL 1154075 (9th Cir. 2025) (en banc), the Ninth Circuit, sitting en banc, found that the allegedly tortious deployment of website tracking cookies by the online payment processing platform Shopify represented the company's ‘expressly aim[ing]’ its conduct at California and thus subjected the company to personal jurisdiction in the state.

In its ruling in *Briskin*, the en banc court both reversed the decision by a three-judge panel of the same court of appeals that affirmed a district court's dismissal for lack of personal jurisdiction and overruled a 2020 Ninth Circuit decision in *AMA Multimedia, LLC v Wanat*, 970 F.3d 120 (9th Cir. 2020) that had required a ‘forum-specific focus’ or ‘differential targeting’ to establish specific personal jurisdiction, finding the rationale for such requirement to be incorrect.

The en banc court's ruling in *Briskin* cited as support a ruling by a different three-judge panel of the Ninth Circuit in *Herbal Brands, Inc. v Photoplaza, Inc.*, No. 21-17001, 2023 WL

4341454 (9th Cir. 2023) that ‘if a defendant, in its regular course of business, sells a physical product via an interactive website and causes that product to be delivered to the forum, the defendant has purposefully directed its conduct at the forum such that the exercise of personal jurisdiction may be appropriate.’

While the en banc court’s ruling in *Briskin* harmonised in the Ninth Circuit the personal jurisdiction standard between sales of physical goods and other online businesses and activities, a split seems to be emerging between the federal circuits with respect to personal jurisdiction over disputes arising out of sales of physical goods. Several circuits – including the Second and Seventh, in addition to the Ninth – appear willing to find that specific jurisdiction applies regardless of the volume of such sales to the applicable forum; in contrast, cases in both the Fifth Circuit and the Eighth Circuit appear to find that jurisdiction applies only in the event that that a threshold volume of sales is achieved.

In a different context – the application of state sales taxes to online sales – the US Supreme Court appeared to endorse an approach similar to that of the Fifth and the Eighth Circuits. In *South Dakota v Wayfair, Inc.* (138 U.S. 2080 (2018)), the Court overturned its half-century old ‘physical presence’ requirement for establishing sales tax nexus, and found that the requirement of the South Dakota law at issue for ‘a merchant to collect the tax only if it does a considerable amount of business in the State’ was sufficient to overcome potential burdens on interstate commerce, which burdens would be particularly onerous for businesses that make only a small volume of sales to customers in the particular state.

Law stated - 31 July 2026

Establishing a business

- 5 | 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?

As a general matter, the regulatory and procedural requirements in the US that govern the establishment of a digital business are substantially similar to the requirements governing the establishment of a brick-and-mortar business. Among other things, both types of business are subject to various licencing and registration requirements, but those requirements typically vary based more on the underlying goods and services rather than on whether the business is digital or brick-and-mortar.

Law stated - 31 July 2026

CONTRACTING ON THE INTERNET

Contract formation

- 6 | 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?

Subject to certain exceptions, legal contracts may be formed digitally. The elements required for the formation of a digital contract are as those for more traditional contracts: mutual assent (ie, 'offer and acceptance'); consideration; mutuality (ie, a 'meeting of the minds'); capacity; and legality. With digital contracts, the element of 'mutual assent' is often more complicated than in the context of more traditional contracts, as the various forms of digital contracts – including 'browsewrap' agreements, 'sign-in wrap' agreements, 'clickwrap' agreements and 'scrollwrap' agreements – present different methods by which the offeree is required to 'accept' the contract.

'Scrollwrap' agreements require the offeree to scroll through the entirety of the contract and to click 'accept' (or similar) to effect acceptance of the terms.

'Clickwrap' agreements require the offeree to click 'accept' (or similar) to effect acceptance of the terms, but do not require the offeree to scroll through the contract.

'Sign-in wrap' agreements expressly notify offerees that the applicable product or service is subject to certain terms, but do not require the offeree to click 'accept' to effect acceptance of such terms.

'Browsewrap' agreements are pursuant to the inclusion on the offeror's digital property of a hyperlink to the applicable terms, and the offeree is deemed to 'accept' those terms by browsing the digital property.

Courts are most likely to find effective 'acceptance', and to enforce, 'scrollwrap' agreements, as they are generally understood to require a clear affirmative act of the offeree that is 'informed'. Courts are also likely to find 'clickwrap' agreements to be enforceable, as they also require a clear affirmative act of the offeree.

'Browsewrap' agreements are least likely to be enforced, as the user may not even be aware that there was an 'offer' made.

Whether 'sign-in wrap' agreements are enforceable will generally hinge on the particular manner in which 'offer' was presented by the offeror and 'acceptance' was deemed effected by the offeree, and such agreements often require courts to undertake a fact-intensive review, although the Fourth Circuit's March 2025 decision in *Dhruva v CuriosityStream Inc.*, No. 24-1080 (4th Cir. 2025) demonstrates that such reviews may yield different conclusions. In *Dhruva*, the Fourth Circuit concluded that the design and content of CuriosityStream's website would have put a reasonably prudent user on notice of the company's contractual offer and reversed a federal district court's decision that had found that the applicable hyperlinked sentence in the 'sign-in wrap' agreement did not expressly constitute the user's agreeing to such contractual terms.

Law stated - 31 July 2026

Applicable laws

- 7 | 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?

Answer in progress.

Law stated - 31 July 2026

Electronic signatures

- 8** | 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?

The Electronic Signatures in Global and National Commerce Act (15 U.S.C. § 7001 et seq) (ESIGN Act) is the primary federal law that recognises and defines electronic signatures. Section 7001(a) of the ESIGN Act provides that, 'with respect to any transaction in or affecting interstate or foreign commerce – (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.' The ESIGN Act requires, for an electronic record to satisfy any requirement that information relating to such transaction be in writing, that the consumer be provided with clear and conspicuous notice in accordance with the provisions of the statute and affirmatively consent to the use of such electronic record (and not withdraw such consent).

Under the ESIGN Act, central elements of the definition of 'electronic signature' include requirements that signature be 'attached to or associated with' the applicable contract or record and the execution or adoption of such signature be 'with the intent to sign the record'.

The ESIGN Act expressly provides that the statute does not apply to certain transactions and documents, including with respect to:

- the creation and execution of wills, codicils, or testamentary trusts;
- adoption, divorce or other matters of family law;
- contracts or records governed by certain provisions of the applicable state's implementation of the Uniform Commercial Code;
- court orders or notices, or official court documents required to be executed in connection with court proceedings; and
- notices of cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities).

The Uniform Electronic Transactions Act (UETA) is a model law published by the Uniform Law Commission that represents the general state law counterpart to the ESIGN Act. UETA has been adopted in some form by 49 US states, plus the District of Columbia, Puerto Rico and the US Virgin Islands; only New York has not adopted UETA, but it enacted legislation – the Electronic Signatures and Records Act (NY State Tech L § 301 et seq) – that is similar in substance to core provisions of UETA.

Although the ESIGN Act's reference to 'validity' is not included, UETA, like the ESIGN Act, provides that: '(a) a record or signature may not be denied legal effect or enforceability

solely because it is in electronic form; and (b) a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.'

Also, like the ESIGN Act, under UETA, central elements of the definition of 'electronic signature' include requirements that (1) such signature be 'attached to or associated with' the applicable record [note that the ESIGN Act's reference to 'contract' is not included in UETA's definition] and (2) the execution or adoption of such signature be 'with the intent to sign the record.'

UETA also expressly provides that its provisions do not apply to a transaction to the extent it is governed by certain laws, including (1) like the ESIGN Act, a law governing the creation and execution of wills, codicils or testamentary trusts and (2) the identical enumerated provisions of the Uniform Commercial Code as those set forth in the ESIGN Act. UETA expressly requires that both parties to the applicable transaction agree to conduct the transaction by electronic means.

A different, and more narrow, uniform state law – the Uniform Computer Information Transaction Act (UCITA) – was initially proposed in 1999, but, due to concerns with that model law, it was adopted by only two states and five states enacted 'bomb-shelter' laws protecting their consumers from provisions of the UCITA.

Law stated - 31 July 2026

Breach

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

Breaches of digital contracts are generally subject to the dispute resolution provisions of the applicable contract, which may provide for litigation or an alternative dispute resolution method such as arbitration or mediation. The acceleration of the digital economy has given rise to an associated increase in disputes regarding digital contracts, and online dispute resolution has emerged as method of addressing such upsurge. In addition, 'on-chain' arbitration – with services provided by a number of specialised platforms – all may resolve disputes for blockchain-based transactions within the same decentralised infrastructure as the underlying contract.

Law stated - 31 July 2026

FINANCIAL SERVICES

Regulation

- 10 | 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?

Answer in progress.

Law stated - 31 July 2026

Electronic money and digital assets

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

Answer in progress.

Law stated - 31 July 2026

Digital and crypto wallets

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

Answer in progress.

Law stated - 31 July 2026

Electronic payment systems

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

Answer in progress.

Law stated - 31 July 2026

Online identity

- 14 | 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?

Answer in progress.

Law stated - 31 July 2026

DOMAIN NAMES AND URLS

Registration procedures

- 15 | 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 Internet Corporation for Assigned Names and Numbers (ICANN) – a multistakeholder, nonprofit public benefit corporation – is responsible for accrediting generic top-level domain (eg, .com, .net, .org, .biz, and .info) registrars and for setting the policies and procedures that govern domain registries for such generic top-level domains. For each of such top-level domains, ICANN has appointed and entered into an agreement with a single official registry organisation, which, among other things, is responsible for maintaining a database of the necessary domain name registration data for such domain.

Registrars are accredited by ICANN, certified by the registries to sell domain names and responsible for registering domain names. They are bound by the Registrar Accreditation Agreement with the applicable ICANN organisation and by their agreements with the registries. Registrar accreditation includes an assessment of financial stability, technical ability, and operational capability. Registrars must be party to a Registrar Accreditation Agreement with ICANN and an agreement with each applicable registry, in addition to their agreements with registrants themselves. As of March 2024, there were approximately 2,800 ICANN-accredited registrars.

Registry Services, LLC manages the .us domain name – the official country code top-level domain for the US within the global domain name system – on behalf of the US Department of Commerce. Use of .us domains are subject to specific marketing guidelines and terms and conditions, described in the .US Brand Identity Guidelines. Registrants for a .us domain name must satisfy one of three nexus category requirements:

- a natural person who is a US citizen, who is a permanent resident of the US or any of its possessions or territories, or whose primary place of domicile is in the US or any of its possessions;
- a US entity or organisation that is incorporated or otherwise organised under the laws of any US state, the District of Columbia, or any of its possessions; or
- a foreign entity with substantial lawful contacts (eg, maintenance of an office or facility) with, or regular lawful activities (eg, selling goods or providing services to customers) within, the US.

Law stated - 31 July 2026

IP ownership

- 16** | 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?

Under US copyright law, there is no protection for domain names. Under certain limited circumstances, a domain name may receive trademark protection, but the criteria for such protection are stringent and most domain names will not satisfy such criteria. To qualify for trademark protection:

- the domain name (1) must be distinctive, either by itself or resulting from consumer association between the domain name and the domain owner and its business (a

'source-identifying characteristic') and (2) must be used on a bona fide basis in the ordinary course of trade ('used in commerce'); and

- the domain name's owner was the first to use such domain name in association with the sale of the associated goods and services ('first use').

The 'source-identification characteristic' condition for 'distinctiveness' under the first criterion was recently affirmed by the US Supreme Court in *United States Patent and Trademark Office v Booking.com B.V.* (140 S. Ct. 2298 (2020)). In ruling that 'booking.com' should not be denied trademark protection as 'generic', the Court held that 'Whether any given 'generic.com' term is generic ... depends on whether consumers in fact perceive that term as the name of a class or, instead, as a term capable of distinguishing among members of the class.'

Although trademark ownership is not necessary to challenge the use or registration of a domain name, ownership of a registered trademark may assist in challenging such use or registration, in particular if the domain name infringes the trademark or dilutes or tarnishes the trademark. The domain name would need to be likely to generate consumer confusion, from a combination of similarity to the trademark and engaging in a business that provides similar goods or services to those of the trademark owner.

Law stated - 31 July 2026

ADVERTISING

Regulation

17 | What rules govern online advertising?

There are myriad US federal and state laws, rules and regulations, as well as self-regulatory codes, that govern online advertising. Many of those laws, rules and regulations – such as the Federal Trade Commission Act (15 U.S.C. § 41 et seq) (FTC Act), the federal Lanham Act (15 U.S.C. § 1051 et seq) (Lanham Act), and state consumer protection laws – govern both offline and online advertising, while others are limited to particular online advertising channels or to particular consumers or industries.

The FTC Act is a federal consumer protection law that, under section 5 of the statute, prohibits unfair or deceptive commercial acts or practices, which include unfair or deceptive advertising and marketing, and under section 12, prohibits the dissemination of any false advertisement for the purpose of inducing, or which is likely to induce, the purchase of food, drugs, devices, services or cosmetics. Under its broad consumer protection enforcement authority, the Federal Trade Commission (FTC) has emerged as the primary federal regulator in the advertising space and online advertising in particular. Within the FTC is a specialised Division of Advertising Practices (DAP), which is tasked with enforcing federal 'truth-in-advertising' laws, including in connection with unfair or deceptive advertising practices under section 5 of the FTC Act.

Particular areas of online advertising that the FTC has specifically addressed in this context are 'online behavioural advertising' (discussed further below) and 'native advertising', which is advertising content that bears a similarity to the articles, entertainment and other material

that surrounds it online. In its December 2015 'Enforcement Statement on Deceptively Formatted Ads', the FTC set forth principles its uses to determine whether an ad format is deceptive and indicated that it would find an advertisement that materially misleads consumers as to its true nature or source (eg, suggesting that it is news or a feature, rather than an ad) to be deceptive, even if the claims in the advertisement itself are truthful and non-misleading. In addition, in July 2023, the FTC issued guidance addressing the application of section 5 of the FTC Act to the use of endorsements and testimonials in advertising, including by influencers and in social media.

In August 2022, pursuant to its authority under section 18 of the FTC Act, the FTC published an advanced notice of proposed rulemaking in respect of a potential Trade Regulation Rule on Commercial Surveillance and Data Security. While not limited solely to online advertising, the advance notice specifically utilised the term 'commercial surveillance' when referring to such online advertising practices as personalised and targeted advertising, appearing to signal a more aggressive approach to online advertising by the FTC. However, the FTC under the current presidential administration has indicated that it has shifted its focus from the underlying business practice to concrete consumer harm.

The Lanham Act also prohibits false or misleading advertisements, but its enforcement mechanism is a private right of action.

Federal laws that are limited to particular online advertising channels or to particular consumers or industries include: the Controlling the Assault of Non-Solicited Pornography and Marketing Act (15 U.S.C. § 7701 et seq) (CAN-SPAM Act), which regulates commercial electronic messages, including email advertising and marketing; the Telephone Consumer Protection Act (47 U.S.C. § 227) (TCPA) and the Telemarketing Sales Rule (promulgated by the FTC under the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. § 6101 et seq)) (TSR), both of which regulate, among other telemarketing activities, text message advertising and marketing; the Children's Online Privacy Protection Act (15 U.S.C. § 1501 et seq) (COPPA), which regulates the online collection of personal information from and about children under the age of 13 and, pursuant to rules promulgated by the FTC, prohibits, without prior verifiable parental consent, both (1) the serving of targeted advertising to a known child and to sites known to be directed primarily to children and (2) the collection of personal information from or about a known child or on a site known to be directed primarily to children.

US states have generally regulated online advertising through their consumer protection laws, including laws that, like the FTC Act (on which many of such laws are modeled), prohibit unfair or deceptive acts or practices. Such laws are primarily enforced by the applicable state's attorney general, and some state consumer protection laws also include a private right of action. In recent years, there have been multiple instances of coalitions of dozens of state attorneys general have filed massive lawsuits claiming that certain online advertising-related practices violated their states' consumer protection laws. One of such lawsuits resulted in a US\$391.5 million settlement by Google with the attorneys general of 40 US states.

Since 2018, 23 US states have enacted general privacy laws, and 22 of such laws expressly provide consumers with the right to opt out of the use of their personal data for targeted advertising based on their activity across non-affiliated digital properties. Since August 2022, California has entered into more than a dozen settlements arising out of alleged California Consumer Privacy Act (CA Civ. Code § 1798.100 et seq) (CCPA) violations, all of

which have included alleged violations of the law's obligations with respect to consumers' right to opt out of the 'sale' or 'sharing' for 'cross-context behavioural advertising' of personal information. Such settlements have included: a US \$12.75 million settlement with General Motors and its Onstar affiliate arising out of various allegations about the companies' personal information use, retention, and disclosure practices, including in connection with failures to provide consumers with required notices and an opportunity to opt out or limit the use of such data; a US\$2.75 settlement with Disney arising out of various allegations about failures to satisfy opt-out requirements mandated by CCPA, including by only partially effectuating consumers' opt-out requests and not implementing them across all of Disney's systems, brands, and devices; a US\$1.55 million settlement with Healthline Media arising out of various allegations, including allegations that the company's opt-out mechanisms did not function properly and that the company failed to test such mechanisms; a US\$1.35 million settlement with Tractor Supply Company arising out of various allegations, including that the company's privacy webform did not opt consumers out of third-party tracking technologies that the company used for advertising purposes (ie, 'sharing' of 'personal information' under CCPA) or inform consumers where or how they could so opt out; and a US\$1.2 million settlement with Sephora arising out of allegations that the company used and disclosed consumers' personal information for advertising and analytics purposes, without providing appropriate notice or opt-out mechanisms or honouring a 'user-enabled global privacy control'). In addition, over the last several years, Texas has significantly accelerated its privacy enforcement, including with respect to the Texas Data Privacy and Security Act (TDPSA), the state's general privacy law, which went into effect in July 2024. In January 2025, Texas filed an action against Allstate and its Arity subsidiary that included claims alleging violations of obligations under TDPSA to provide consumers with disclosures regarding the companies' targeted advertising practices and a method to opt out of such targeted advertising. And in December 2025, the state filed separate lawsuits against five smart TV manufacturers, alleging that their 'Automated Content Recognition' (ACR) data collection practices were unlawful and constituted violations of TDPSA; the state subsequently entered into settlements with two of the smart TV manufacturers and secured a temporary restraining order against a third.

Numerous states – including California, Florida, Maryland, and Washington – plus the District of Columbia have also enacted email advertising laws that include prohibitions similar to those of the CAN-SPAM Act. There has been a recent surge in class action litigation claims alleging violations of several of such laws, in particular California's "Restrictions of Unsolicited Commercial Email Advertisers" law and Washington "Commercial Electronic Mail Act".

In addition to the myriad federal and state laws, rules and regulations, online advertising practices may also be subject to codes, principles, guidelines, policies and/or procedures of one or more of myriad self-regulatory organisations, including:

- The self-regulatory principles of the Digital Advertising Alliance (DAA), a consortium of leading US national marketing and advertising trade groups;
- The Principles & Self-Regulatory Framework of the Network Advertising Initiative (NAI), a self-regulatory association comprised exclusively of companies engaged in 'data-driven, digital advertising involving interoperable exchanges of personal data used for or derived from the selection, delivery and measurement of such advertising' (Network Advertising);

- The Mobile Advertising Guidelines of the MMA, a global marketing trade association; and
- The policies and procedures of BBB National Programs, including with respect to its National Advertising Division and its Children's Advertising Review Unit.

Law stated - 31 July 2026

Targeted advertising and online behavioural advertising

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

The FTC Act does not expressly require companies to have or disclose a privacy policy; however, the FTC has taken the position that, if company publishes a privacy policy, it must reflect the company's actual information practices, and the FTC may bring enforcement actions against companies that have unfair or deceptive information practices. Taken together, the FTC likely would consider a company's failure to disclose in its privacy policy the collection and disclosure of data for online behavioural advertising and other targeted advertising to constitute an unfair or deceptive act or practice under section 5 of the FTC Act. In addition, the FTC published 'Self-Regulatory Principles for Behavioral Advertising' in 2009 and expanded the self-regulatory programme to the mobile environment in 2015.

In 2023, the FTC entered into separate seven-figure settlements with two different consumer-focused digital healthcare platforms, BetterHelp and GoodRx, arising out of alleged violations of section 5 of the FTC Act, as well as the FTC's Health Breach Notification Rule (16 C.F.R. § 318) (Health Breach Notification Rule) under Health Insurance Portability and Accountability Act (Public Law 104-191), in connection with such platforms' targeted advertising activities, including the deployment of third-party advertising companies' pixels on their websites. In 2024, the FTC accelerated its efforts in this area, as demonstrated by its:

- entering into a US\$16.5 million settlement with a software provider that included prohibitions on the company's sale of browsing data for advertising purposes, including the targeted advertising practices alleged in the FTC's complaint;
- entering into multiple settlements with data providers that imposed substantial injunctive relief, including in connection with targeted advertising practices; and
- in the wake of such settlements, announcing in a blogpost that 'Browsing and location data are sensitive. Full Stop.'

Such de facto characterisation of 'browsing' data as 'sensitive' represented a significant expansion not only of the FTC's prior public positioning, including the proposed settlements described in the blogpost, but also as compared to any US state general privacy law enacted to date.

However, the change of presidential administration in early 2025 and resultant changes in the constitution of the FTC seem to have reversed that expansion, with the current FTC evincing less scepticism of targeted advertising generally and a greater focus on the roles of both economics and 'cognizable harm' in consumer protection analyses. In

a September 2024 statement, current FTC Chair (and then-FTC Commissioner) Andrew Ferguson indicated that he did 'not share the...view that the display of targeted advertising to adults is, on balance, harmful. (Targeted advertising to children and teenagers is another matter entirely.)'

COPPA, which regulates the online collection of personal information from and about children under the age of 13 and, pursuant to rules promulgated by the FTC, prohibits, without prior verifiable parental consent, both (1) the serving of targeted advertising to a known child and to sites known to be directed primarily to children and (2) the collection of personal information from or about a known child or on a site known to be directed primarily to children.

Since 2018, 23 US states have enacted general privacy laws, and 22 of such laws expressly provide consumers with the right to opt out of the use of their personal data for targeted advertising based on their activity across non-affiliated digital properties. In addition, a majority of such laws impose heightened obligations -- typically opt-in consent, but in certain instances, such as under the laws of Connecticut and Maryland, outright prohibitions -- on targeted advertising to certain teenagers over the age of 13 (with the threshold age for such obligations ranging from 15 to 18, depending on the state law).

Several of the self-regulatory principles and guidance documents of the DAA govern online behavioural advertising and other targeted advertising, including the DAA's 'Self-Regulatory Principles for Online Behavioral Advertising', 'Self-Regulatory Principles for Multi-Site Data', and 'Application of Self-Regulatory Principles to the Mobile Environment'. The Principles & Self-Regulatory Framework of the NAI govern Network Advertising, a term that, under the NAI's binding principles, 'may include activities that support 'sales,' 'shares,' 'cross-context behavioral advertising' or similar practices as defined by applicable laws in the United States.'

Law stated - 31 July 2026

Misleading advertising

19 | Are there rules against misleading online advertising?

Section 5 of the FTC Act prohibits unfair or deceptive commercial acts or practices, which include materially misleading advertising and other unfair or deceptive advertising and marketing activities, and section 12 of the FTC Act prohibits the dissemination of any false advertisement for the purpose of inducing, or which is likely to induce, the purchase of food, drugs, devices, services or cosmetics. A 'false advertisement' is an advertisement, other than labelling, that is misleading in a material respect.

One particular area that the FTC has specifically addressed in the context of misleading online advertising is 'native advertising', which is advertising content that bears a similarity to the articles, entertainment, and other material that surrounds it online. In its December 2015 'Enforcement Statement on Deceptively Formatted Ads', the FTC set forth principles its uses to determine whether an ad format is deceptive and indicated that it would find an advertisement that materially misleads consumers as to its true nature or source (eg,

suggesting that it is news or a feature, rather than an ad) to be deceptive, even if the claims in the advertisement itself are truthful and non-misleading.

Under the 'prior substantiation doctrine' utilised by the FTC, an advertiser must have a 'reasonable basis' standard for each of its material advertising claims, and failure to have such a reasonable basis can result in an FTC Act claim. The 'reasonable basis' standard depends on a number of factors, including: the type of claim, the product (for example, the standard may be higher for health and safety claims, for which the FTC requires a high level of substantiation, including 'competent and reliable scientific evidence'), the consequences of a false claim, the benefits of a truthful claim, the cost of developing substantiation for the claim, and the amount of substantiation that experts in the field believe is reasonable.

State consumer protection laws that, like the FTC Act (on which many of such laws are modelled), prohibit unfair or deceptive acts or practices, including materially misleading advertising. While such laws are primarily enforced by the applicable state's attorney general, some state consumer protection laws also include a private right of action. Notably, however, courts have generally rejected the application of the prior substantiation doctrine by consumers in class action litigation alleging violations of state consumer protection laws.

The CAN-SPAM Act prohibits senders of commercial emails – any electronic mail message whose primary purpose is to advertise or promote a commercial product or service – from using any false or misleading header information or subject lines that would likely mislead a recipient about a material fact regarding the message's contents or subject matter. Numerous states – including California, Florida, Maryland, and Washington – plus the District of Columbia have enacted laws that include similar prohibitions, and there has been a recent surge in class action litigation claims alleging violations of several of such laws, in particular California's "Restrictions of Unsolicited Commercial Email Advertisers" law and Washington "Commercial Electronic Mail Act".

Law stated - 31 July 2026

Restrictions

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

Subject to the general rule that illegal products and services may not be advertised online, there are no US laws that expressly prohibit the advertising of specific products or services, including particular digital products or services. However, online platforms, digital properties and other service providers often have their own policies that include prohibitions or restrictions with respect to certain products or services, including digital products and services such as cryptocurrency-related products and services (eg, exchanges) and online gambling.

Law stated - 31 July 2026

Direct email marketing

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

The CAN-SPAM Act regulates commercial electronic messages, including email advertising and marketing, while the TCPA and the TSR both regulate, among other telemarketing activities, text message (including SMS) advertising and marketing.

The CAN-SPAM Act requires commercial emails – any electronic mail message whose primary purpose is to advertise or promote a commercial product or service – to include:

- accurate and non-misleading routing and header information;
- a subject line that is not deceptive;
- clear and conspicuous notice that the recipient has the right to opt out of receiving future email messages from the sender, and instructions on how to opt out
- an internet-based opt-out mechanism capable of receiving opt-out requests for at least 30 days after message transmission (and the sender must honour an opt-out request within 10 business days); and
- clear and conspicuous indication that the email is an advertisement or solicitation, unless the recipient has affirmatively consented to receive commercial emails; and
- the sender's physical postal address.

Both the TCPA (including the regulations promulgated under it) and the TSR regulate the collection and use of telephone numbers for commercial purposes, apply to telephone calls and text messages (the TCPA also applies to faxes), and set forth rules governing, among other things:

- times during the day when telephone solicitations can be made;
- use of automated telephone equipment for solicitations;
- maintenance of a national 'Do-Not Call Registry'; and
- information the solicitor must give to the consumer.

The Federal Communication Commission enforces the TCPA and its regulations and has authority to prescribe regulations under the TCPA. The FTC has authority to prescribe rules and regulations under the Telemarketing and Consumer Fraud and Abuse Prevention Act and to enforce such rules and regulations, including the TSR. Both the TCPA and the Telemarketing and Consumer Fraud and Abuse Prevention Act (under which the TSR was promulgated by the FTC) permit private rights of action. However, the TSR's private right of action applies only if the amount in controversy exceeds US\$50,000 in actual damages for each person adversely affected by the telemarketing activities, a limitation that does not apply to the TCPA's, which provides for recovery of either actual or statutory damages ranging from US\$500 to US\$1,500 per unsolicited call or message. Because of the potential for massive statutory damages, TCPA class action litigation is a key issue for businesses, and the terms of the statute are frequently litigated.

Under each state general privacy law, both email addresses and telephone numbers constitute personal data and are therefore subject to 'purpose limitation' requirements (if any) under each such law. (All but two of the 23 state general privacy laws enacted to date include 'purpose limitation' requirements.) Therefore, an email address or a telephone number collected for a particular specified purpose (eg, for the controller to contact a consumer in connection with a transaction) may not be able to be used for direct marketing

unless, among other things, the controller also discloses the marketing purpose at the time of collection of such information.

In addition, numerous states – including California, Florida, Maryland, and Washington – plus the District of Columbia have enacted laws that, like the CAN-SPAM Act, prohibit senders of commercial emails from using any false or misleading header information or subject lines that would likely mislead a recipient about a material fact regarding the message's contents or subject matter. There has been a recent surge in class action litigation claims alleging violations of several of such laws, in particular California's "Restrictions of Unsolicited Commercial Email Advertisers" law and Washington "Commercial Electronic Mail Act".

Law stated - 31 July 2026

ONLINE PUBLISHING

Hosting liability

- 22** | 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?

Internet service providers, telecommunications providers and other 'interactive computer service' providers (and users) are generally immune from liability for third-party content that they merely host and display, pursuant to section 230(c) of the Communications Act (47 U.S.C. § 151 et seq) (Communications Act) (added pursuant to Title V [the Communications Decency Act] of the Telecommunications Act), which provides that 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'. Section 230(c) also expressly exempts such parties from liability on account of 'any action voluntarily taken in good faith to restrict access' to certain 'objectionable' material. However, if such parties engage in activities that render them 'internet content providers', in particular through the creation or development of content, they would not be able to avail themselves of the protections of section 230 with respect to such content, so avoiding those activities would help to minimise liability. In addition, such parties must also provide a notification to customers about the availability of parental control protections at the time they enter into agreements with customers.

Section 230(e) expressly provides that the statute's protections are limited and that the immunity it provides does not extend to certain other laws, including federal criminal statutes, intellectual property laws, state laws or the Electronic Communications Privacy Act (Public Law 99-508). However, in connection with such intellectual property law limitation, Title II [Online Copyright Infringement Liability Limitation] of the Digital Millennium Copyright Act (Public Law 105-304) added a new section 512 to the federal Copyright Act to create a separate set of liability protections for online service providers. Under subsections (a)-(c) of such section, a service provider is not liable for copyright infringement with respect to material that it transmits, routes or provides connections for, caches or stores at the direction of users, in each case as long as the service provider satisfies certain enumerated conditions.

In 2025, the chairs of both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) expressed their respective opinions that, while section 230 may provide broad immunity when platforms make content available, such broad protection should not necessarily extend to platforms' removal of content. Although in February 2025 the FTC issued a request for public comments regarding restrictive measures by platforms, to date neither the FTC nor the FCC has put their expressed opinions into regulatory action, through rulemaking or enforcement.

Law stated - 31 July 2026

Content liability

- 23** | 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?

Answer in progress.

Law stated - 31 July 2026

Shutdown and takedown

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

Under section 230(c) of the Communications Act – which is intended to provide ‘protection for ‘good Samaritan’ blocking and screening of offensive material’ – an internet service provider or telecommunications provider may voluntarily shut down a web page containing defamatory or other ‘objectionable’ material provided by a third party without court authorisation, even if such material is constitutionally protected. To avail itself of such protections under section 230, such provider must take such action in good faith and, in connection with such defamatory material, must be acting solely in its capacity as an ‘interactive computer service’ provider rather than as an ‘internet content provider’. However, in 2025 the current chairs of both the FCC and the FTC expressed their respective opinions that the broad immunity of section 230 should not necessarily extend to platforms' removal of content.

Law stated - 31 July 2026

INTELLECTUAL PROPERTY

Data and databases

- 25** | Are data and databases protected by IP rights?

Under US law, copyright protection is afforded to 'original works of authorship fixed in any tangible medium of expression' (17 U.S.C. § 102(a)). The US Supreme Court has found that for a work to be 'original', it must have been 'independently created by the author' and 'possess at least some degree of creativity' (see *Feist Publications, Inc. v Rural Tel. Serv. Co.*, 499 U.S. 340, 346 (1991)). As data itself 'lacks the modicum of creativity necessary to transform mere selection into copyrightable expression' (see *Feist* at 363), it is not subject to US copyright protection. However, as 'factual compilations', databases may be copyrightable, if the choices as to selection and arrangement of such databases – for example, 'which facts to include, in what order to place them, and how to arrange the collected data so that they can be used effectively' – entail the modicum of creativity sufficient to denote originality.

Law stated - 31 July 2026

Third-party links and content

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

Neither US federal or state law prohibits a website, digital platform or other online content provider from linking to third-party websites, platforms or content, although the applicable third party may impose restrictions on such linking in its terms of service. However, the absence of prohibitions under the US legal framework does not insulate a party that engages in such linking from liability.

Title II [Online Copyright Infringement Liability Limitation] of the Digital Millennium Copyright Act (Public Law 105-304) (DMCA) added a new section 512 to the federal Copyright Act to create a series of limitations on liability for copyright infringement by online service providers. Under subsection (d), a service provider is not liable for linking to an online location only if it, among other things:

- does not have actual knowledge of infringement and, in the absence of actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; and
- upon obtaining such knowledge or awareness, or being notified as to claimed infringement, acts expeditiously to disable access to the applicable material (17 U.S.C. § 512(d)).

Law stated - 31 July 2026

- 27** | 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?

Use of a third party's content by the owner or operator of a website, digital platform, or other online content provider, without permission from the third party, may give rise to liability under both US copyright law and US trademark law.

Under US law, copyright protection is afforded to 'original works of authorship fixed in any tangible medium of expression' (17 U.S.C. § 102(a)), although the federal Copyright Act sets forth a series of limitations on exclusive rights, including 'fair use' (17 U.S.C. § 107). The statute's 'fair use' exception establishes a balancing test, consisting of the following four factors to be considered: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The burden is on the party using or seeking to use the copyrighted material to prove 'fair use'. However, the failure of the copyright owner to consider the issue of fair use prior to issuing a takedown notice under the Digital may constitute the 'bad faith' necessary to demonstrate a 'misrepresentation' under the federal Copyright Act (see *Lenz v Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008)).

Under US law, the standard for determining trademark infringement requires a determination that use of the trademarked material is likely to cause consumer confusion, and courts typically apply a multi-factor test to make such determination. In addition to an infringement claim, use of third-party content without permission may also result in a claim that such usage dilutes or tarnishes the trademark.

Law stated - 31 July 2026

Metaverse and online platforms

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

The distributed nature of a blockchain-based metaverse creates challenges with enforcing US intellectual property rights. Section 512 of the federal Copyright Act, added pursuant to the DMCA:

- provides a 'takedown notice' mechanism for a copyright owner to provide notice of a copyright infringement claim to a service provider; and
- establishes an exemption from infringement liability for a service provider that stores infringing content on a system or network controlled or operated by or for the service provider if, among other things, upon learning of infringement or being notified as to claimed infringement, it acts expeditiously to disable access to the material (17 U.S.C. § 512).

However, one of the core elements of a blockchain is distributed technology, pursuant to which information is stored not on a single service provider's system or network, but across many different servers. In addition, once content is stored on a blockchain, it cannot be deleted or changed.

Law stated - 31 July 2026

Exhaustion of rights and first-sale doctrine

.

- 29** | 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?

The US recognises both the 'exhaustion doctrine' with respect to patent rights and the 'first-sale doctrine' with respect to copyright and trademark rights. The general rule under such doctrines is that, following the lawful sale of a patented, copyrighted or trademarked product, the exclusive rights of the intellectual property owner to control the use and sale of such product are 'exhausted' and the purchaser may resell that product.

However, in *Capitol Records, LLC v ReDigi Inc.*, 910 F.3d 649 (2d Cir. 2018), the Second Circuit affirmed the district court's decision, holding that the defendant/appellant's resale of a digital music file did not constitute the sale of a product (which is subject to the 'first-sale doctrine' codified as a limitation on exclusive rights in section 109(a) of the federal Copyright Act), but instead constituted the making of at least one unauthorised reproduction (which is not subject to such limitation on exclusive rights). The Second Circuit's decision both (1) referenced the US Copyright Office's conclusion, following a multi-year evaluation, that '§ 109 does not apply to otherwise unauthorised digital transmissions of a copyrighted work, reasoning that such transmissions cause the recipient to obtain a new copy of the work' and (2) distinguished sales that constitute a reproduction of a digital work from sales of a physical product that contains digital material, but left some ambiguity, as the court declined to 'decide whether *all* digital file transmissions over the Internet make reproductions' and noted that 'other technology may exist or be developed that could lawfully effect a digital first sale.'

Law stated - 31 July 2026

Administrative enforcement

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

Answer in progress.

Law stated - 31 July 2026

Civil remedies

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

In the US, intellectual property (IP) owners have a variety of potential civil remedies, including monetary damages, injunctive relief, and other remedial actions pursuant to court orders. Monetary damages can consist of actual damages, which are intended to compensate the IP owner for the injury suffered on account of the infringement, or, if elected by the IP owner in the case of copyright or trademark infringement, statutory damages provided by the applicable statute. Under both copyright law and trademark law, statutory

damages are higher for wilful infringement and, under patent law, courts may 'treble' actual damages in the event the patent infringement is found to be wilful. In IP cases, a court may issue both injunctions, ordering the infringing party to cease its use of the applicable intellectual property, and other remedial orders, including directing the seizure or destruction of infringing materials.

Law stated - 31 July 2026

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

32 | 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?

Although there is no federal general privacy law, the first draft of federal general privacy legislation in two years – the Securing and Establishing Uniform Rights and Enforcement over Data Act (SECURE Data Act) – was released in April 2026. In its initial draft form, the SECURE Data Act's definition of 'personal data' generally aligns with corresponding definitions under state general privacy laws.

Under the 23 state general privacy laws that have been enacted to date, 'personal data' (or 'personal information', the term under the California Consumer Privacy Act (CA Civ. Code § 1798.100 et seq) (CCPA)) generally means 'any information that is linked or reasonably linkable to an identified or identifiable' resident of the applicable state, although, among other things, exclusions from the applicable definition vary across such laws. Through July 2026, the 23 states that have enacted general privacy legislation are:

Currently effective (as at 7/1/2026):

- California;
- Virginia;
- Colorado;
- Connecticut;
- Utah;
- Texas;
- Oregon;
- Montana;
- Iowa;
- Delaware;
- New Hampshire;
- Nebraska;
- New Jersey;
- Tennessee;

- Minnesota;
- Indiana;
- Kentucky; and
- Rhode Island.

Not yet effective:

- Oklahoma (effective 1/1/2027);
- Louisiana (effective 1/1/2027);
- Alabama (effective 5/1/2027); and
- Vermont (effective 1/1/2028).

The only one of such state general privacy laws that applies to personal information of individuals acting in a commercial or employment capacity is CCPA.

Each of such state general privacy laws includes provisions with respect to 'sensitive data' (or 'sensitive personal information'). All but three of such laws require affirmative 'opt-in' consent to process sensitive data; the three outliers – the general privacy laws of Utah and Iowa and, somewhat surprisingly, CCPA – impose 'opt-out' obligations with respect to sensitive data. The Maryland Online Data Privacy Act, which went into effect in October 2025, imposes the strictest obligations of such laws, including by: (1) requiring the collection and processing of sensitive data to be strictly (not just reasonably) necessary to provide or maintain a specific product or service requested by the applicable consumer; (2) prohibiting the sale of sensitive data; and (3) with respect to consumers that a controller 'knew or should have known' to be under the age of 18, prohibiting not only the sale of such consumers' personal data, but also the processing of such consumers' personal data for targeted advertising.

Since June 1, 2025, three states -- Virginia, Connecticut, and Oregon -- amended their general privacy laws to prohibit the sale of precise location data; Oregon's amendment also prohibited the sale of personal data of a consumer whom the controller actually knew to be under the age of 16 (or wilfully disregarded that fact). In addition, on June 30, 2026, New Jersey amended its general privacy law to prohibit the sale of sensitive data.

The definition of 'sensitive data' varies across such state general privacy laws, but common elements typically include personal data that:

- reveals a consumer's racial or ethnic background, religious beliefs, mental or physical health condition or diagnosis, or sexual orientation; or
- is genetic or biometric data (often qualified by whether such data is processed for the purpose of uniquely identifying an individual), precise geolocation data (typically, a radius of approximately one-third of a mile), or a child's personal data.

CCPA's definition of sensitive personal information includes several additional elements, including a consumer's social security, driver's license, state identification card, or passport number and a consumer's account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account.

In addition, while not a general privacy law and despite its narrow-sounding title, the Washington My Health My Data Act (WA MHMDA) is a broad law that imposes a series of obligations and prohibitions with respect to the collection, processing, and sharing of 'consumer health data'.

WA MHMDA defines 'consumer health data' expansively to mean 'personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status', and sets forth a lengthy, non-exhaustive list of items that constitute 'physical or mental health status'. Notably, a proposed amendment to exclude from the definition of 'consumer health data' information about a consumer's purchase or use of everyday items (eg, 'athletic and sports equipment', 'groceries, food, and beverages', and 'over-the-counter dietary supplements' failed to make it into the final version of WA MHMDA.

Under WA MHMDA, a 'regulated entity':

- may not 'collect' consumer health data except to the extent necessary to provide a product or service requested by the consumer from the regulated entity or with 'consent' for such collection for a specified purpose;
- may not 'share' consumer health data except to the extent necessary to provide a product or service requested by the consumer from the regulated entity or with 'consent' for such sharing (separate and distinct from the consent for collection); and
- may not 'sell' or offer to sell consumer health data without first obtaining 'valid authorization' (separate and distinct from any consent for collection or sharing), which must be signed and dated by the consumer and contain certain enumerated provisions.

Law stated - 31 July 2026

Registration and appointment of data protection officer

- 33** | 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?

As a general matter, parties that process personal data are not required to register with a regulator to engage in such processing activities. However, a limited number of US states – California, Texas, Vermont Oregon, and, beginning 1 January 2027, Connecticut – require 'data brokers' to register annually with the applicable regulator and pay an annual fee. Further, in an accelerated process at the end of its most recently concluded fiscal year, New Jersey enacted a law, effective 30 June 2026, that (1) imposes annual registration requirements not only on 'data brokers', but also on 'data collectors' engaged in the selling or licensing of personal data, and (2) establishes a tiered fee structure under which the annual registration fee can be as much as US\$1.5 million, if the volume of personal data sold or licensed satisfies the highest threshold; less than two weeks after enactment, with questions surrounding the law, the state's Division of Consumer Affairs published an alert indicating that the first registration window would open on 1 April 2027

and that it would provide additional guidance on the law's requirements, including with respect to registration. In addition, approximately two-thirds of US states, plus the District of Columbia, impose legal requirements on telemarketers to obtain a licence before engaging in telemarketing calls into or from those states.

Among the federal laws:

- under the Health Insurance Portability and Accountability Act (Public Law 104-191) (HIPAA): a 'covered entity' is required to designate a 'privacy officer' and to identify a 'security officer', in each case responsible for the covered entity's development and implementation of the applicable required policies and procedures; and a 'business associate' is required to identify a 'security officer' responsible for the business associate's development and implementation of the required security policies and procedures; and
- under the FTC's Safeguards Rule promulgated under the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq) (GLBA), each covered 'financial institution' must designate a 'qualified individual' to implement and supervise the organisation's information security programme.

Law stated - 31 July 2026

Extraterritorial issues

- 34** | 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?

Although, as noted previously, there is currently no federal general data protection law, such federal laws governing data protection as the Federal Trade Commission Act (15 U.S.C. § 41 et seq) (FTC Act), the GLBA, and HIPAA are generally understood to apply only to activities within the United States and/or territories thereof. In an antitrust context (rather than a data protection context), the Federal Trade Commission (FTC) (in conjunction with the US Department of Justice) has released guidance to reinforce the principle that remedies should avoid extraterritorial application unless necessary to effectively redress harm or threatened harm to US commerce and consumers.

The obligations under state general privacy laws apply to organisations based on applicable territorial requirements and thresholds, including:

- requirements that the organisation either conduct business within the particular state or either target goods or services to residents of the particular state or produce goods or services consumed by residents of the particular state; and
- thresholds based on the number of affected 'consumers' within the particular state.

Accordingly, organisations need not have a physical place of business or employees within a particular state for that state's general privacy law to impose obligations on the organisations. In contrast, rights of individuals under state general privacy laws – for example, the 'right to delete' personal data, the 'right to access' personal data, the 'right to correct' personal data, and the 'right to opt out' from the sale of personal data or the use

of personal data for targeted advertising – are afforded only to residents of the particular state.

Law stated - 31 July 2026

Bases for processing

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

US laws generally don't require organisations to assert a legal basis for the processing of personal data or the exporting or transferring of personal data. However, the FTC has taken the positions that: if a company publishes a privacy policy, it must reflect the company's actual information practices; and a company that revises its privacy policy should obtain consumers' affirmative 'opt-in' consent before using their data in ways that are materially different from what was set forth in the privacy policy that was in effect when the company collected it.

For the first time in 2023, US state general privacy laws began imposing obligations with respect to the principle of 'purpose limitation', which requires that personal data be collected and processed only for the specific purposes disclosed to the consumer and prohibits the controller from processing personal data for purposes that are not reasonably necessary for or compatible with such disclosed purposes, unless the controller first obtains the consumer's 'opt-in' consent to the processing of personal data for such secondary purposes. Of the 23 state general privacy laws enacted to date, only those of Utah and Iowa do not include purpose limitation restrictions. Notably, among the allegations underlying both the California attorney general's May 2026 US\$12.75 million settlement with General Motors and its Onstar affiliate and the California attorney general's July 2025 US\$1.55 million settlement with Healthline Media were violations of CCPA's purpose limitation obligations, rising out of the failure to disclose sales of personal information and insufficient disclosures regarding sharing of personal information for targeted advertising, respectively.

Law stated - 31 July 2026

Data export and data sovereignty

- 36** | 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?

While US federal and state laws generally do not impose rules or restrictions with respect to the export or transfer of personal data to other jurisdictions, one significant exception is the Final Rule on 'Preventing Access to Americans' Bulk Sensitive Data and United States Government Data by Countries of Concern' (Bulk Sensitive Data Final Rule), which

was promulgated by the National Security Division of the Department of Justice under a February 2024 executive order and went into effect in April 2025.

The Bulk Sensitive Data Final Rule's regulations prohibit or otherwise restrict US persons from knowingly engaging in certain 'covered data transactions', including transactions of government-related data or 'bulk' sensitive personal data', with a 'country of concern' – currently deemed to be each of China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Venezuela – or a 'covered person' (either an individual or entity) under the control of a country of concern.

The Bulk Sensitive Data Final Rule expressly provides that it is intended to 'counter the unusual and extraordinary threat to US national security posed by the continuing efforts of certain countries of concern to access and exploit' such data, and, among other things, calls out certain key risks, including those presented by the data broker industry and by the development of AI and other advanced technologies.

It should be noted that US regulators may not view data sovereignty or data localisation rules as necessary due to the broad rights afforded with respect to data to the US government under the USA PATRIOT Act (Public Law 107-56) (Patriot Act) and the Clarifying Lawful Overseas Use of Data Act (Public Law 115-41).

Law stated - 31 July 2026

Sale of data to third parties

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

The FTC Act does not expressly prohibit selling or transferring personal information to third parties. However, if a company's privacy policy includes statements regarding the company's selling and/or transfer practices, it must comply with them. This includes situations where the privacy policy states that the company will not sell, share, or otherwise disclose personal data to third parties.

The FTC has used section 5 of the FTC Act to charge companies that fail to comply with their own privacy policies and has also stated that it is a violation of the FTC Act for a company to retroactively change its privacy policy without providing data subjects an opportunity to opt out. In addition, the FTC may bring enforcement actions against companies that have unfair or deceptive information sharing practices, even if those companies do not have a privacy policy or have not violated their privacy policies.

Subject to limited enumerated exceptions, the Bulk Sensitive Data Final Rule promulgated under Executive Order 14117 of February 28, 2024 prohibits 'covered data transactions' involving sales or other 'data brokerage' with a 'country of concern' or 'covered person'.

Pursuant to Regulation P promulgated under the GLBA, a 'financial institution' may not share an individual's 'nonpublic personal information' with a nonaffiliated third party without providing the individual the right to opt out, unless:

- the disclosure is to a third party that uses the information to perform services for the financial institution;

- the financial institution and the third party enter into a contract that requires the third party to maintain the information's confidentiality and use the information only for the prescribed purpose; and
- the financial institution provides initial notice of its privacy practices to the individual before sharing the information (12 C.F.R. § 1016.13).

The FTC's Safeguards Rule promulgated under the GLBA also imposes requirements for safeguards when sharing individuals' information with service providers (16 C.F.R. § 314.4).

HIPAA generally requires covered entities to obtain an individual's written consent before using or disclosing their protected health information (PHI) to third parties. However, the HIPAA Privacy Rule allows covered entities to disclose PHI to business associates if the parties enter into an agreement that requires the business associate to use the information only for the purposes for which it was engaged by the covered entity, safeguard the information from misuse, and help the covered entity comply with its duties under the Privacy Rule (45 C.F.R. §§ 164.502, 164.504).

US state privacy laws do not expressly prohibit selling or transferring personal data to third parties. However, each of the state general privacy laws enacted to date requires any 'controller' (or 'business', under CCPA) that 'sells' a consumer's personal data or processes a consumer's personal data for 'targeted advertising' (or 'sharing' personal information, under CCPA) to: clearly and conspicuously disclose such selling and processing activities, as well as the manner in which a 'consumer' may exercise the right to 'opt out' of such activities; and provide consumers the right to opt out of the 'sale' of their personal data and the use of their personal data for 'targeted advertising' (or 'sharing' personal information, under CCPA), although the right to opt out of such use for targeted advertising is not expressly provided by Utah's law.

The meaning of 'sale' varies across such state laws, with a relatively small subset of such laws limiting the consideration provided under the definition to 'monetary' consideration, while the standard under a majority of such laws is 'monetary or other valuable' consideration. Subject to limited exception under CCPA, such opt-out rights do not extend to the transfer of personal data to 'processors' (or 'service providers', under CCPA) that may process such personal data solely on behalf of the 'controller' (or 'business', under CCPA) and pursuant to a written contract that sets forth certain requirements in accordance with the applicable laws.

In addition, under Nevada's data broker law (NV Rev. Stat. §603A), consumers have the right to opt out of sales of their 'covered information', which, under such law, constitutes a subset of what is generally considered personal data or information.

Sales, sharing or similar transfers of personal data about users of an online service or digital platform are generally subject to the applicable terms and conditions between the transferor controller and the transferee third party. A substantial majority of state general privacy laws expressly provide that a party to such a transfer will not be liable in the event of the other party's violation of the applicable law; with respect to a transferor controller, such exclusion is predicated on such controller's not having actual knowledge that the transferee third party would violate the applicable law.

CCPA is unique among state general privacy laws in that it:



- requires the sale or sharing of personal information to or with a third party to be pursuant to an agreement between the controller and the third party that includes certain enumerated provisions, including obligations on the third party to comply with applicable obligations under CCPA and to provide the same level of privacy protection with respect to the personal information; and
- imposes substantial obligations on third parties, including with respect to providing 'Notice at Collection' and further selling or sharing of the personal information it receives from the transferor controller.

Law stated - 31 July 2026

Consumer redress

- 38** | 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?

Federal laws

None of the FTC Act, the GLBA or the HIPAA provides individuals with a private right of action. However, other federal laws governing privacy provide for a private right of action, including:

- The Telephone Consumer Protection Act (47 U.S.C. § 227) which provides for recovery of either actual or statutory damages ranging from US\$500 to US\$1,500 per unsolicited call or message;
- The Telemarketing Sales Rule (promulgated by the FTC under the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. § 6101 et seq)) (TSR), although such private right of action applies only if the amount in controversy exceeds \$50,000 in actual damages for each person adversely affected by the telemarketing activities; and
- The Video Privacy Protection Act (18 U.S.C. § 2710), which governs the disclosure and destruction of 'personally identifiable information' concerning any 'consumer' by 'video tape service providers' and has been the subject of a recent wave of class action litigation relating to the use of third-party technology on websites and other digital properties that play videos. In January 2026, the US Supreme Court granted certiorari in *Salazar v Paramount Global*, No. 25-459 to resolve a split among federal circuit courts regarding who constitutes a 'consumer' under the statute, although the Court has declined to address a circuit split with respect to what constitutes the disclosure of 'personally identifiable information'. A decision in *Salazar* is generally expected in early 2027.

State laws

CCPA is the only effective or enacted state general privacy law that provides consumers with a private right of action. Although the section of CCPA providing such private right of action is entitled 'Personal Information Security Breaches' and a California legislative summary noted that the statute 'provides a limited private right of action for data breaches', several recent federal district court decisions in the Northern District of California seem to have taken a more expansive view of the law's private right of action. In each of *M.G. v Therapymatch, Inc.*, No. 23-cv-4422, 2024 WL 4219992 (N.D. Cal. September 16, 2024), *Shah v Capital One Financial Corp.*, No. 24-cv-05985-TLT, 2025 WL 714252 (N.D. Cal. March 3, 2025), and *Allison v PHH Mortgage Corp.*, No. 3:25-cv-05323-RFL (N.D. Cal. 14 May 2026), the plaintiff alleged that the defendant's use of customary website tracking technologies (eg., third-party cookies) constituted disclosure to, and unauthorised access by, third parties of personal information, and the district court found that such allegation sufficiently stated a CCPA section 150 claim.

Despite the customary absence of a private right of action, state general privacy laws typically provide consumers with the following rights:

- 'Right to delete' personal data;
- 'Right to access' personal data;
- 'Right to correct' personal data [the law of Iowa is the only outlier that does not expressly provide such a right];
- 'Right to data portability';
- 'Right to opt out' of:
 - Sale of personal data;
 - Use of personal data for targeted advertising (or sharing of personal information, under CCPA) [the law of Iowa is the only outlier that does not expressly provide such an opt-out right]; and
 - Use of personal data for 'profiling' in furtherance of decisions that produce legal or similarly significant effects concerning the consumer [the laws of Utah and Iowa are the only outliers that do not provide such an opt-out right]; and
- 'Right to non-discrimination' for exercising any of the consumer rights contained in such law.

The definition of 'consumer' under each of such state general privacy laws is limited to an individual who is a resident of the applicable state.

WA MHMDA not only provides individuals with the rights to access and/or delete their consumer health data and to withdraw consent from a regulated entity's collection and/or sharing of their consumer health data, but also provides consumers with a private right of action. The first class action lawsuit setting forth claims under WA MHMDA was filed in February 2025, and a second was filed in November 2025.

WA MHMDA's private right of action originates under Washington state's consumer protection act, as any violation of WA MHMDA is expressly deemed to constitute both an 'unfair or deceptive act in trade or commerce' and 'unfair method of competition' for purposes of such consumer protection act. In a similar vein, other state consumer

protection acts have been invoked by attorneys general in connection with personal data processing activities, both in states that have enacted general privacy laws and in states that have not enacted general privacy laws (eg, New York); each state consumer protection act provides individuals with a private right of action.

In addition, a host of 20th century 'anti-wiretap' laws that require 'all-party' consent provide private rights of action that have been the basis for a recent wave of class action litigation, particularly with respect to the California Invasion of Privacy Act (California Penal Code § 630 et seq) and increasingly under other state laws such as Pennsylvania's Wiretapping and Electronic Surveillance Control Act (18 PA Cons Stat § 5701 et seq) and Florida's Security of Communications Act (Fla. Stat. ch. 934), arising out of the processing of personal data via the deployment of third-party cookies and other online technologies.

Law stated - 31 July 2026

Non-personal data

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

In the US, there is no single, comprehensive federal data protection law. Most federal privacy laws and regulations are generally sector and activity-specific, with the FTC Act being a notable exception. While such sector and activity-specific laws, such as the GLBA and HIPAA, generally regulate a subset of personal data (eg, non-public personal information in the case of GLBA, and 'protected health information' in the case of HIPAA), the application of the FTC Act – a federal consumer protection law that prohibits unfair or deceptive commercial acts or practices – may be broader. Such an unfair or deceptive act or practice with respect to non-personal data could technically fall under the FTC Act, although, as the FTC has long applied the statute and its rules to business practices that affect consumer privacy and data security, use of non-personal data is generally less likely to implicate significant privacy or security issues.

Law stated - 31 July 2026

DOCUMENT DIGITISATION AND RETENTION

Digitisation

40 | 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?

While parties are generally not required to retain documents in original paper form, there is a limited number of specialised rules that require certain documents to be so retained. For example, under section 4.703(c) of the Federal Acquisition Regulation (Title 48 of the CFR) require federal contractors and subcontractors to retain 'original records' for at least one year after imaging to permit periodic validation of the applicable imaging systems.

Law stated - 31 July 2026

Retention

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

Various federal and state laws, rules, and regulations stipulate minimum retention periods for certain documents and records, with obligations and retention periods varying based on the applicable law, the type of document or record, and the nature and size of the applicable business. For example, the Recordkeeping and Reporting Requirements under Title VII of the Civil Rights Act (42 U.S.C. § 2000e), the Americans with Disabilities Act (42 U.S.C. § 12117), and the Genetic Information Nondiscrimination Act (42 U.S.C. § 2000ff-6) require any personnel or employment record made or kept by an employer with 15 or more employees to be retained for a period of one year from the date of the making the record or of the personnel action involved, whichever occurs later, and any personnel records of an employee who was involuntarily terminated to be retained for a period of one year following the date of termination (29 CFR § 1602.14); however, the corresponding retention periods imposed by such requirements on institutions of higher learning are two years (29 CFR § 1602.49). Other laws, rules and regulations mandate substantially longer retention periods for applicable documents. In addition, the model Uniform Preservation of Private Business Records Act – which has been adopted in some form by such states as Texas, Illinois and Colorado – provides that, unless another law, rule or regulation applicable to particular business record prescribes a different retention period or procedure for disposal, a business subject to the particular statute may destroy such business record after three years from the date of creation.

Law stated - 31 July 2026

DATA BREACH AND CYBERSECURITY

Security measures

- 42** | 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?

As a general rule, companies must implement and maintain reasonable security procedures and practices appropriate to the nature of the particular information, and the Federal Trade Commission (FTC) has used the Federal Trade Commission Act's (15 U.S.C. § 41 et seq) prohibition on unfair or deceptive acts or trade practices to bring actions against companies that fail to do so. This general requirement contemplates different measures based on the underlying data – for example, 'reasonableness' with respect to payment cards would necessitate compliance with the applicable requirements of the Payment Card Industry Data Security Standard (PCI DSS), while it would not be reasonable to require such security measures to protect less sensitive data.

Numerous activity and sector-specific federal laws, rules and regulations impose more detailed and tailored cybersecurity obligations, including:

- the FTC's Safeguards Rule promulgated under the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq) (GLBA), which requires covered companies to: develop, implement and maintain a written information security programme with administrative, technical and physical safeguards appropriate for the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the applicable data; and designate a qualified individual to implement and supervise such information security programme;
- the Interagency Guidelines Establishing Information Security Standards pursuant to the Federal Deposit Insurance Act (12 U.S.C. § 1831p-1), the GLBA, and the Fair Credit Reporting Act (15 U.S.C. § 1681), which requires each 'insured depository institution' to implement a comprehensive written information security programme that includes administrative, technical and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities, and sets forth standards both for developing and implementing such safeguards and with respect to the proper disposal of consumer information; and
- the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 C.F.R. Parts 160 and 164) (Security Rule), which requires 'covered entities' and 'business associates' to:
 - implement and maintain administrative, technical and physical safeguards and satisfy organisational requirements, including to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic 'protected health information' and
 - designate a security officer responsible for the development and implementation of the policies and procedures required by the Security Rule.

Many states have adopted laws setting forth security obligations in line with the general rule described above, to implement and maintain reasonable security measures to protect personal information from unauthorised access, acquisition, destruction, disclosure, modification or use. Notably, the only private right of action provided under the state general security laws enacted to date is the limited right under California Consumer Privacy Act (CA Civ. Code § 1798.100 et seq), which right extends to certain security breaches resulting from a business's violation of its duty to implement and maintain reasonable security procedures and practices.

The first recommendation of the California Data Breach Report issued by the state's Department of Justice in 2016 provided that the 'Center for Internet Security's Critical Security Controls define a minimum level of information security that all organisations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organisation's environment constitutes a lack of reasonable security.' While the CIS Controls remain a commonly used set of cybersecurity standards, it is unclear whether satisfying such standards, without more, would be deemed by California (or other) regulators to constitute 'reasonableness'.

In addition to the CIS Controls, other commonly used cybersecurity standards include the National Institute of Standards and Technology's Cybersecurity Framework and the ISO/IEC 27000 family of standards jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Certain states have also enacted activity or sector-specific laws, rules or regulations with respect to data security, including: approximately 25 state laws based on the National Association of Insurance Commissioners Insurance Data Security Model Law; and the New York State Department of Financial Services' 'Cybersecurity Requirements for Financial Services Companies' (23 NYCRR 500), which regulations were significantly amended in November 2023 to enhance a number of its requirements to address 'the ever-growing threat posed to information and financial systems by nation-states, terrorist organisations, and independent criminal actors.'

Law stated - 31 July 2026

Data breach notification

43 | 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?

In addition to laws imposing data security obligations, all 50 states, plus the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands, have effective data security breach notification laws with respect to certain personal information. All businesses, including digital businesses, are subject to such laws. Each of such state data security breach notification laws includes requirements for the applicable entity to notify affected consumers, although such notice requirements are typically subject to certain enumerated exceptions. Approximately two-thirds of such laws also require the applicable entity to notify the state's attorney general or another specified regulatory authority.

There are also data breach notification obligations under certain activity or sector-specific state laws, rules, and regulations, including:

- state laws modelled on the National Association of Insurance Commissioners Insurance Data Security Model Law, which requires 'Licensees' to notify consumers as required by the applicable state's general data security breach notification law and to notify the chief insurance regulatory official of the applicable state as promptly as possible (but in no event later than 72 hours after a determination that a 'Cybersecurity Event' has occurred); and
- the New York State Department of Financial Services' (NYDFS) 'Cybersecurity Requirements for Financial Services Companies' (23 NYCRR 500), pursuant to which a covered entity must notify the superintendent of the NYDFS 'as promptly as possible' (but not more than 72 hours after a determination that a cybersecurity incident has occurred).

Various activity and sector-specific federal laws, rules and regulations also include breach notification requirements, including:

- the Safeguards Rule promulgated under the GLBA, which requires covered companies to report 'notification events' to the FTC within 30 days of discovery of the notification event;
-

the Interagency Guidelines Establishing Information Security Standards pursuant to the Federal Deposit Insurance Act (12 U.S.C. § 1831p-1), GLBA, and the Federal Credit Reporting Act (15 U.S.C. § 1681), which, as part of the comprehensive written information security programmes required to be implemented by 'insured depository institutions', provides guidance on 'response programs' that should be developed and implemented to address unauthorised access to or use of customer information that could result in substantial harm or inconvenience to a customer. This includes procedures to notify the applicable federal regulator and, in certain situations, appropriate law enforcement authorities;

- under HIPAA:
 - HHS's Breach Notification Rule (45 CFR § 164.400 et seq), which requires 'covered entities' and 'business associates' to notify affected patients, the Secretary of HHS, and, in certain circumstances, the media in the event of a breach of unsecured 'protected health information'; and
 - the FTC's Health Breach Notification Rule, which requires 'vendors of personal health records and related entities' to notify affected patients, the FTC, and, in certain circumstances, the media in the event of a breach of unsecured 'individually identifiable health information' that is in a personal health record maintained or offered by such vendor or related entity; and
- the Securities and Exchange Commission's final rule (FR. Doc. 2023-16194) adding Item 1.05 [Material Cybersecurity Incidents] to current reports on Form 8-K (or Form 6-K, for foreign private issuers) and requiring registrants to:
 - file such a current report within four business days after determining that a 'cybersecurity incident' is material, which report must describe the material aspects of the nature, scope, and timing of the incident and the incident's material impact or reasonably likely material impact on the company, including its financial condition and results of operations; and
 - determine whether a cybersecurity incident is material without undue delay after discovery of the incident'; materiality can be either quantitative/financial or qualitative.

Law stated - 31 July 2026

Government interception

- 44** | 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?

The Fourth Amendment to the United States Constitution, which prohibits governmental authorities from conducting 'unreasonable searches [or] seizures', applies to federal, state and local governments. The combination of the nature and sensitivity of the data (eg, basic user registration data or complete email logs) and the type of request or demand (eg, a subpoena or a warrant based on 'probable cause') produced by the authority typically

determines whether access is 'reasonable' or 'unreasonable' and whether a company should produce any or all of the requested data to the authority.

In one recent case, *Carpenter v United States*, 138 S. Ct. 2206 (2018), the US Supreme Court found that the Federal Bureau of Investigation's (FBI) warrantless accessing and acquiring from a wireless carrier the cell phone record data of an individual invaded that individual's reasonable expectation of privacy and constituted a search that violated the Fourth Amendment. And in a case decided at the end of the 2025-26 term, *Chatrue v United States*, 609 U.S. (2026), the Court (a) citing *Carpenter*, found that police officers conducted a Fourth Amendment search when they accessed an individual's historical cell phone location information, even if the materials obtained were handed over by a third-party technology company, and (b) remanded the case to the circuit court, in particular to determine whether, at each stage of the search process, the underlying geofence warrant 'satisfied the Fourth Amendment's requirements of particularity and probable cause'.

A potential loophole to such Fourth Amendment jurisprudence has emerged in recent years, as governmental authorities have purchased personal data, including sensitive personal information (eg, location data), from third-party data brokers without a warrant, court order or similar request. In July 2023, separate bipartisan-sponsored bills – each entitled the 'Fourth Amendment is Not for Sale Act' – were introduced in the US Senate and the US House of Representatives, to address and close such loophole by amending 18 U.S.C. § 2702, a section of the Electronic Communications Privacy Act (Public Law 99-508). The House bill passed the US House of Representatives in April 2024, but it stalled in the US Senate. Similar bills -- the 'Government Surveillance Reform Act' and the 'Surveillance Accountability Act' -- were introduced in Congress in the first half of 2026, but to date neither has advanced significantly. In contrast, in May 2025, Montana became the first US state to enact a law substantially similar to the Fourth Amendment is Not for Sale Act bills; subject to limited exceptions, such Montana law prohibits government entities from purchasing certain data, including precise geolocation data and contents of electronic communications, other than pursuant to a warrant or subpoena.

More specifically, certain federal laws and measures with the force of law – notably, Section 702 of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq) (FISA 702), the Patriot Act, Executive Order 12333 (United States Intelligence Activities), and Presidential Policy Directive 28 (Signals Intelligence Activities) (PPD-28) – permit the collection of certain content and information under specific circumstances, particularly for intelligence and national security purposes. The permissions afforded by the framework of such laws and measures have been central to decisions issued by the Court of Justice of the European Union that invalidated European Commission (EC) adequacy determinations with respect to multiple trans-Atlantic data protection frameworks between the EU and the US, first the US-EU Safe Harbor Framework (invalidated in 2015) and subsequently the EU-US Privacy Shield Framework (invalidated in 2020). It is expected that the third trans-Atlantic data protection framework to receive an EC adequacy determination – the EU–US Data Privacy Framework – will be challenged on similar grounds. The statutory authorisation of FISA expired in June 2026, although, even without an extension or re-authorisation (to date, there has been neither), it will continue to operate until March 2027 under a recertification issued earlier in 2026 by the US Foreign Intelligence Surveillance Court.

Law stated - 31 July 2026

GAMING

Legality and regulation

- 45** | 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?

It is permissible to operate online betting and gaming businesses within the US, but only in certain states and subject to the applicable laws, rules, and regulations of those states and of the federal government. Currently, online sports betting is legal in approximately 30 states and the District of Columbia, while online casino gambling is legal in eight states (in addition to Nevada, where internet poker is legal but other online casino games are not).

Online sports betting has expanded rapidly since the US Supreme Court held in *Murphy v. National Collegiate Athletic Association*, 138 S. Ct. 1461 (2018) that the 'anti-authorization' provision of the federal Professional and Amateur Sports Protection Act (PASPA) – which made it unlawful for a governmental agency, including a state governmental agency, to authorise sports gambling – violated the US Constitution's 'anti-commandeering' principle and, as the other provisions of PASPA were not severable, PASPA itself was unconstitutional.

Although legal age for most forms of offline gambling in a majority of US states where gambling is permitted is 18; for online betting or gaming the minimum age is typically 21, for both sports and non-sports online betting (in a handful of states, the minimum age for online sports betting is 18). Prospective online betting customers are required to verify their age and identity in the registration process.

Law stated - 31 July 2026

Cross-border gaming

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

Although sports betting may be authorised by all US states after US Supreme Court's decision in *Murphy v National Collegiate Athletic Association*, 138 S. Ct. 1461 (2018), such betting is limited by the Federal Wire Act (18 U.S.C. § 1084) (Wire Act), a 1961 criminal statute that prohibits the use of a 'wire communication facility' for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placement of wagers'. Even though the Wire Act is more than six decades old, its broad definition of 'wire communication facility' has been found to cover internet communications. Accordingly, intrastate online sports betting – where the operator and the bettor are in the same US state – is legal under the Wire Act in states that authorise such betting, but the Wire Act is generally understood to prohibit interstate online sports betting.

For about half a century, the US Department of Justice (DOJ) took the position that the Wire Act applied to all betting, not just sports betting. However, in 2011, the DOJ issued a memorandum opinion (2011 DOJ Opinion) reversing that position and indicating that the Wire Act was limited only to sports betting and therefore did not apply to other forms of betting or gaming, such as state lotteries and online casinos. The 2011 DOJ Opinion was sandwiched between two federal Court of Appeals decisions – that of the Fifth Circuit in *In re Mastercard Intern. Inc.*, 313 F.3d 257 (5th Cir. 2002) and that of the First Circuit in *N.H. Lottery Comm’n v Rosen*, 986 F.3d 38 (1st Cir. 2021) – that each found that the Wire Act applied only to sports gambling, not other forms of gambling, and, accordingly, interstate and foreign online non-sports gambling is not prohibited by such statute.

Rules in the US with respect to gambling in a metaverse, however, are still rife with uncertainty, including on account of complexities with respect to applicable laws and jurisdiction. In addition, given the application of the Wire Act to online sports betting, distributed nature of a blockchain-based metaverse renders sports gambling in such a metaverse extremely challenging, if not impossible, to conduct in compliance with such statutes, as the operator would need to be ensure not only that all bettors are in the same state as the operator, but also that all data associated with bets or wagers is stored on ledgers in that state as well.

Law stated - 31 July 2026

OUTSOURCING

Key legal issues

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

Answer in progress.

Law stated - 31 July 2026

Sector-specific issues

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

Answer in progress.

Law stated - 31 July 2026

Contractual terms

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

Answer in progress.

Law stated - 31 July 2026

Employee rights

- 50** | 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?

Answer in progress.

Law stated - 31 July 2026

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

- 51** | 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?

Although there is currently neither federal nor state comprehensive artificial intelligence (AI) legislation, there are various federal and state laws – both general and sector-specific – that regulate the use of AI, automated decision-making, and profiling.

Federal

The January 2025 Trump Initial AI Policy Framework Executive Order specified that "[i]t is the policy of the United States to sustain and enhance America's global AI dominance" and directed the suspension, revision, or rescission of actions inconsistent with such policy, reflecting the current presidential administration's prioritisation of AI leadership and focus on removing rules and restrictions that it views as inhibiting the country's competitive position." In a similar vein, the version of the 2025 federal 'One Big Beautiful Bill Act' (Public Law No. 119-21) that initially passed the US House of Representatives would have imposed, subject to limited exceptions, a 10-year moratorium on state and local enforcement of AI laws and regulations. Although the US Senate voted overwhelmingly to remove such moratorium provision from the version of the law that was ultimately enacted, the White House's 'Ensuring a National Policy Framework for Artificial Intelligence' executive order (December 2025) (Trump Subsequent AI Policy Framework Executive Order) -- which built on the Trump Initial AI Policy Framework Executive Order in providing that "[i]t is the policy of the United States to sustain and enhance [its] global AI dominance through a minimally burdensome national policy framework for AI" -- (a) directed the US Attorney General to establish an AI Litigation Task Force 'to challenge [s]tate AI laws inconsistent with [such] policy'; and (b) directed the US Secretary of Commerce to issue a Policy Notice providing that 'states with onerous AI laws are ineligible' for portions of the

approximately US\$21 billion in 'non-deployment funds' under the November 2021 federal Broadband Equity, Access, and Deployment (BEAD) Program.

While both of such 2025 AI Policy Framework Orders espoused a deregulatory approach to AI, the White House's June 2026 'Promoting Advanced Artificial Intelligence Innovation and Security' executive order represented a domain-specific departure from that overarching policy, in particular by directing multiple agencies to create a 'voluntary framework' for AI developers with respect to 'covered frontier models'. Under such framework, AI developers would be able to engage and collaborate with the federal government and provide the federal government with access to covered frontier models before they are released.

Although a joint statement issued in April 2023 by four federal agencies – the Consumer Financial Protection Bureau, the Department of Justice, the Equal Employment Opportunity Commission (EEOC), and the FTC – highlighted instances where such agencies had engaged in formal actions under long-standing federal laws and regulations to address potentially harmful uses of automated systems, the policy set forth in the Trump Initial AI Policy Framework Executive Order, and subsequently reinforced by the Trump Subsequent AI Policy Framework Executive Order, will likely result in a significantly less active regulatory enforcement approach to AI and other automated technologies. In May 2025, FTC Chair Andrew Ferguson signalled such a shift, testifying to a US House committee that the agency would address problems with AI and other new technologies 'as they arise' rather than prospectively.

One high-profile instance in which a federal agency during the second Trump administration continued AI-related enforcement action brought under the Biden administration was the Department of Justice's antitrust lawsuit against RealPage and six property management companies alleging that the provision and use of RealPage's algorithmic rental pricing software -- which was alleged to pool and utilise competitors' confidential data to generate coordinated price recommendations -- constituted violations of the Sherman Antitrust Act (15 U.S.C. §§ 1-7) (Sherman Act), including under the theory that RealPage and its algorithmic software were the 'hub' of a 'hub-and-spoke conspiracy'. While, as of 31 August 2026, the DOJ had entered into settlements with RealPage and four of the property management companies, the DOJ enforcement action remained active against the remaining two property management companies.

State

Twenty-one of the 23 state general privacy laws enacted to date include obligations with respect to 'profiling', which is typically defined by such laws as 'any form of automated processing performed on personal data to evaluate, analyse, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements'.

Twenty of those 21 enacted state general privacy laws – those of Virginia, Colorado, Connecticut, Texas, Oregon, Montana, Delaware, New Hampshire, Nebraska, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky and Rhode Island (all of which are currently effective), as well as those of Alabama, Louisiana, Oklahoma, and Vermont – contain provisions substantially similar to the following: providing 'consumers' with the right to opt out of profiling 'in furtherance of decisions that produce legal or similarly significant effects concerning the consumer'; and requiring 'controllers' to conduct and document a

data protection assessment with respect to 'processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

- unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- financial, physical, or reputational injury to consumers;
- a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
- other substantial injury to consumers.'

A 21st state general privacy law – the California Consumer Privacy Act (CA Civ. Code § 1798.100 et seq) (CCPA) – directs the issuance of regulations with respect to automated decision-making technology, including profiling (ADMT). In July 2025, the California Privacy Protection Agency adopted such regulations, which went into effect on January 1, 2026 (with later compliance dates for certain obligations). The adopted regulations (1) include provisions with respect to consumers' rights to opt out of, and access information about, a business's use of ADMT for a significant decision concerning a consumer and to appeal a business's use of ADMT for such a significant decision, (2) obligate businesses to conduct a risk assessment prior to using ADMT for a significant decision concerning a consumer or for certain other automated processing activities, and (3) require businesses that develop ADMT and make such ADMT available to another business for a significant decision concerning a consumer to provide to the recipient-business all available information that is necessary for the recipient-business to conduct its risk assessment.

In addition to state general privacy laws, numerous states have enacted AI-specific legislation, the broadest of which is the Connecticut Artificial Intelligence Responsibility and Transparency Act (Public Act No. 26-15) (CART Act) which was enacted in May 2026 and will go into effect on October 1, 2026. The CART Act covers a range of AI technologies and elements, including 'automated employment-related decision technology', 'artificial intelligence companions', 'frontier models', 'generative artificial intelligence systems', and 'synthetic data', and sets forth various disclosure obligations, consumer rights, and, with respect to 'large frontier developers', internal safety and governance requirements.

Prior to the CART Act, the broadest AI-specific law was arguably the Texas Responsible Artificial Intelligence Governance Act (Tex. Bus. & Com. Code Ann. § 551.001 et seq) (TRAIGA), which went into effect in January 2026. TRAIGA prohibits the development and/or deployment of an 'artificial intelligence system' for various purposes, including intentionally to manipulate human behaviour in a manner that causes harm or intentionally to unlawfully discriminate against a protected class, and establishes a novel AI regulatory sandbox programme for the testing of artificial intelligence systems, which programme requires applicants to include an impact assessment. Both Utah and Maine have enacted narrower AI-specific legislation focused on transparency, and those laws went into effect in 2024 and 2025, respectively.

Notably, in 2024, Colorado passed the Colorado Artificial Intelligence Act (CAIA), which was signed into law by the state's governor with expressed reservations and was the broadest state-specific legislation enacted at the time. However, in 2026, in its second attempt to address the governor's concerns, the Colorado legislation replaced CAIA with the Automated Decision-Making Technology Act (Senate Bill 26-189) (ADMT Act),

which will go into effect on January 1, 2027. Whereas CAIA was especially focused on 'high-risk artificial intelligence systems', including protecting consumers from risks of 'algorithmic discrimination' arising from the use of such AI systems', the ADMT Act: (a) extends to any 'automated decision-making technology' that is used to materially influence a 'consequential decision' about a consumer relating to such domains as education, employment, housing, financial and lending services, insurance, health care, and essential government services and public benefits; and (b) with respect to such 'covered ADMT', imposes disclosure obligations on both developers and deployers and provides consumers with various rights, including the rights to access and correct personal data used in a consequential decision resulting in an 'adverse outcome' and the right to obtain 'meaningful human review' and reconsideration of such consequential decision.

In addition, three of the most populous US states -- California, New York, and Illinois -- have passed laws requiring 'large' developers of 'frontier' AI models (a)(a) to write, implement, and conspicuously publish a safety, security, and risk management framework (or 'protocol' under New York's law) that governs the large developer's practices with respect to such frontier models, including to identify and mitigate the potential for 'catastrophic risks' and to identify and respond to 'critical safety incidents', and (b) to review and, as appropriate, update such framework at least annually. All three laws also impose additional disclosure obligations on large frontier developers, including an obligation to report to the applicable state agency any critical safety incident pertaining to one or more of its frontier models within a statutorily mandated time period. In addition, both California's law and Illinois' law include whistleblower protections for 'covered employees', and Illinois' law also requires large frontier developers to undergo an annual independent compliance audit. California's law went into effect on January 1, 2026, while both New York's law and Illinois' law will go into effect on January 1, 2027.

Further, state consumer protection laws, in particular those laws that are modelled on the FTC Act, may be applicable to the development and use of AI, and there are also a handful of activity or sector-specific state and local laws governing the use of AI, automated decision-making, and/or profiling, including:

- the Illinois Artificial Intelligence Video Interview Act (Public Law 101-0260) (2020) and New York City's Local Law 2021/144 (2021), each of which sets forth obligations (including with respect to notice and, under Illinois' law, consent) with respect to the use of automated decision-making tools for employment screening of job applicants; New York City's law also includes notice obligations with respect to the use of such tools for employment and promotion screening of employees, while, effective January 1, 2026, another Illinois statute -- the Illinois Human Rights Act (775 ILCS 5/) -- was amended to render it illegal to fail to provide notice regarding the use of any employment-related AI and/or to use any employment-related AI that has a discriminatory effect;
- Colorado's Senate Bill 21-169 (2021), which prohibits insurers from using any algorithms or predictive models that use 'external consumer data and information sources' in a way that unfairly discriminates based on race, colour, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, gender expression; and
- more than a dozen effective or enacted laws set forth obligations with respect to AI technology that is designed to simulate human conversations and interactions

('conversational AI'), including a half-dozen effective or enacted laws -- including effective laws in California (SB 243) and New York (N.Y. Gen. Bus. Law Article 47, §§ 1700-1704) – governing 'AI companion' technology, a subset of conversational AI that is designed to simulate a sustained human-like relationship with the user.

Numerous state attorneys general, either as a coalition or independently, currently have active enforcement pending against RealPage and various property owners/managers alleging that the provision and use of RealPage's algorithmic rental pricing software violated not only the Sherman Act, but also state antitrust laws and state consumer protection laws. A multidistrict class action litigation with similar claims is also currently pending.

Long-standing employment-related legislation has also been used as the basis for class action litigation in connection with the use of AI tools, as in a case (*Baker v CVS Health Corporation*, 1:23-cv-11483 (D. Mass.)) that was settled in 2024 after a federal district denied CVS's motion to dismiss for failure to state a claim. The plaintiff in *Baker* alleged that he participated in an interview that utilised automated interview and application software to assess and screen candidates in violation of a decades-old Massachusetts law (Mass. Gen. Laws ch. 149 § 19B) that, with very narrow exceptions, prohibits an employer or employment agency from administering or requesting to administer a lie detector test to an employee or job applicant and requires all applications for employment to contain a written notice advising applicants that it is 'unlawful in Massachusetts to require or administer a lie detector test as a condition of employment or continued employment.'

Law stated - 31 July 2026

IP rights

- 52** | 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?

Putting aside general intellectual property (IP) laws, rules and regulations, there are few US federal or state rules specifically governing intellectual property and artificial intelligence or machine learning.

US Copyright Office

Since early 2023, the US Copyright Office has been engaging in a broad initiative regarding the intersection of copyright and AI, the first output of which was March 2023 guidance that applied the 'human authorship requirement' to works containing AI-generated material and indicated that, while it would undertake further examination of the application of the law in this area, 'what matters [for copyrightability] is the extent to which the human had creative control over the work's expression and 'actually formed' the traditional elements of authorship'. Pursuant to such guidance:

-

if AI technology receives solely a prompt from a human and produces complex written, visual or musical works in response, the resulting work is not copyrightable, as the traditional elements of authorship are determined and executed by the technology, not the human user; but

- if a human selects, arranges or modifies AI-generated material in a sufficiently creative way, the resulting work and/or such modifications may be copyrightable.

Subsequently, the US Copyright Office released a multi-part 'Report on Copyright and Artificial Intelligence'.

- Part 1 (Digital Replicas) was published in July 2024 and, among other things, recommended the adoption of a new federal law on account of its conclusion that 'existing laws do not provide sufficient redress for those harmed by unauthorized digital replicas'. One of the bills referenced in Part 1, the federal 'TAKE IT DOWN Act', was enacted in May 2025 as Public Law 119-12. The TAKE IT DOWN Act addresses one of the digital replica contexts discussed in the report by imposing a series of obligations and prohibitions with respect to nonconsensual 'intimate visual depictions', including images and videos generated or edited using AI (deepfakes).
- Part 2 (Copyrightability), which was published in January 2025, (a) addressed the copyrightability of outputs created using generative AI, (b) indicated that the determination of copyrightability of a work created using AI, like that of a work created without it, requires a fact-specific consideration, (c) confirmed the position in the March 2023 guidance that content entirely generated by AI cannot be protected by copyright, and (d) affirmed that 'existing principles of copyright law are flexible enough to apply' to generative AI technology.
- A pre-publication version of Part 3 (Generative AI Training) was released in May 2025, addressed the use of copyrighted works in the development of generative AI systems, and concluded that, although 'the use of copyrighted works to power current generative AI systems may be unprecedented in scope and scale, the existing legal framework can address it as in prior technological revolutions.' In such conclusion, the Office specifically referenced the ability of the fair use doctrine to flexibly accommodate new technologies. Notably, the Office has stated that no substantive changes are expected in the final version of the document, and, as of the end of July 2026, the Office's website still includes only the pre-publication version.

Litigation

In the two months following the issuance of the US Copyright Office's March 2023 guidance (and prior to the issuance of any of the parts of the Office's 'Report on Copyright and Artificial Intelligence'), the US Supreme Court both issued an opinion that may, in the absence of additional rules, further complicate the intersection of AI and copyright, and denied certiorari on an appeal of a 2022 decision of the US Court of Appeals for the Federal Circuit in *Thaler v Vidal*, 43 F.4th 1207 (Fed. Cir. 2022) that held that the Patent Act (U.S.C. Title 35) requires an 'inventor' to be a natural person and, therefore, the plaintiff's AI system could not be listed as the inventor on a patent application. (In a subsequent copyright case involving the same plaintiff, in 2026 the Court also denied certiorari on an appeal of a 2025 decision of the US Court of Appeals for the D.C. Circuit in *Thaler v Perlmutter*, 130 F.4th

1039 (D.C. Cir. 2025) that held that the Copyright Act (U.S.C. Title 35) protects only "original works of authorship" and therefore requires an "author" to be a human being, including those who make work for hire.)

In the 2023 copyright opinion, *Andy Warhol Foundation for the Visual Arts, Inc. v Goldsmith*, 598 U.S. 508 (2023), the Court appeared to narrow the 'fair use' defence to copyright infringement in holding that 'transformative use' must be weighed against how the copy is used (eg, in a commercial manner targeting the same market, such as licensing prints to a magazine). The Court's focus on 'transformative use' (rather than just a transformation of the work itself) may be relevant for companies that train their AI systems on content 'scraped' from the internet and use the output for commercial purposes that might be deemed to compete with the sources of such content.

In addition, since the public launch of ChatGPT at the end of November 2022, there have been numerous high-profile IP infringement lawsuits brought by content creators and owners against leading generative AI companies in connection with such companies' training of their AI models, including suits filed by:

- the Authors Guild on behalf of *Game of Thrones* author George RR Martin and more than a dozen other authors against OpenAI, alleging copyright infringement under the Copyright Act (17 U.S.C. § 101 et seq), which suit was consolidated with 11 other cases into a multi-district litigation in April 2025;
- Getty Images against Stability AI, alleging copyright infringement and other violations under the federal Copyright Act and trademark infringement and dilution and unfair competition under the Lanham Act, trademark dilution violations of the Delaware Trademark Act (6 Del. C. § 3301 et seq), and deceptive trade practices in violation of Delaware's Uniform Deceptive Trade Practices Act (25 Del. C. § 2531 et seq.);
- Disney Enterprises and other entertainment companies against Midjourney, alleging copyright infringement under the federal Copyright Act;
- each of The New York Times Company and a collection of other news organisations against Microsoft and OpenAI, alleging:
 - copyright infringement under the federal Copyright Act (17 U.S.C. § 101 et seq);
 - violations of the DMCA on account of the removal of copyright-management information;
 - common law unfair competition by misappropriation;
 - trademark dilution under the Lanham Act; and
 - under the collection of newspapers publishers' claim, dilution and injury to business reputation under section 360-I of the New York General Business Law;
- a coalition of almost three dozen publishing companies, representing nearly 400 newspapers, also alleging copyright infringement under the federal Copyright Act and violations of the DMCA against Microsoft and OpenAI; and
-

the independent music and licencing platform Jamendo against Nvidia, alleging copyright infringement under the federal Copyright Act, as well as breach of contract for violation of the platform's Terms of Use.

Beginning in the second half of 2025, several settlements were reached in major copyright lawsuits against AI developers, including a \$1.5 billion settlement in *Bartz et al. v Anthropic PBC*, No. 3:24-cv-05417-WHA (N.D. Cal.) and a confidential settlement of an approximately US\$621 million lawsuit brought in *UMG Recordings, Inc. et al. v Internet Archive*, No. 3:23-cv-06522-MMC (N.D. Cal.). Prior to settlement, the district court in *Bartz* held that, although the use of the books at issue to train Anthropic's Claude AI and other specific large language models "was exceedingly transformative and was a fair use under Section 107 of the Copyright Act", training AI on pirated copies of such works (as was alleged) that had been downloaded to create a permanent, general-purpose library did not fall under such fair use exception. In July 2026, the *Bartz* settlement, which provides for approximately US\$3,100 per book, received final judicial approval.

To mitigate litigation risks and regulatory uncertainty, AI companies and other companies engaged in training AI models have been entering into, or seeking to enter into, content licensing agreements or other compensation arrangements with media companies and content creators.

Law stated - 31 July 2026

Ethics

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

Federal

While the core principles set forth in the October 2023 Biden AI Executive Order included provisions with respect to the ethical development of AI systems and protection against unlawful discrimination and abuse resulting from the deployment of AI systems, that executive order was revoked by the January 2025 Trump Initial AI Policy Framework Executive Order, which provided that 'engineered social agendas' represented a barrier to American AI leadership. A later executive order, issued in July 2025, directed federal agencies to procure only large language models that 'do not manipulate responses in favour of ideological dogmas such as' diversity, equity, and inclusion. And the December 2025 Trump Subsequent AI Policy Framework Executive Order referred to Colorado's now-superseded CAIA's ban on "algorithmic discrimination" as "requiring entities to embed ideological bias within models".

Although (1) there are already existing federal laws and regulations that apply to discrimination deepened or caused by AI and other automated systems and (2) formal federal regulatory actions have previously addressed potentially harmful uses of automated systems, the current presidential administration has shifted the federal regulatory framework from ethics and potential risks to actual harms.

State

Both of the two broadest AI-specific state laws enacted to date -- Connecticut's CART Act and Texas's TRAIGA -- include provisions with respect to discrimination, although the two laws follow significantly different approaches. The CART Act focuses on discriminatory effect, providing that use of an 'employment-related decision technology' shall not constitute a defence against a complaint alleging a violative discriminatory practice; under the CART Act, evidence of anti-bias testing or a similar effort may be considered by a court (ie, as an intent not to discriminate). In contrast, TRAIGA focuses on discriminatory intent, prohibiting the development and/or deployment of an 'artificial intelligence system' with the intent to unlawfully discriminate against a protected class. Notably, TRAIGA expressly provides that a 'disparate impact is not sufficient by itself to demonstrate an intent to discriminate.'

Law stated - 31 July 2026

TAXATION

Online sales

- 54** | Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

Sales and use taxes in the US are governed by the various states and the District of Columbia, and a majority of states impose tax on the sale of digital products and online services. Whether a sale to a consumer in a particular state is subject to such tax is determined based on whether the seller has a 'nexus' with that state. While having a 'physical presence' in a statute is sufficient to establish nexus, in *South Dakota v Wayfair, Inc.*, 138 US 2080 (2018), the US Supreme Court held that a 'physical presence', though sufficient, was not necessary to establish sales tax nexus and undertaking a considerable amount of business in a state was also sufficient to establish such nexus.

Law stated - 31 July 2026

Server placement

- 55** | 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?

Placing a server in a particular state is generally considered to constitute a 'physical presence' in that state, which would establish sufficient nexus for sales tax purposes and potentially for income tax purposes as well.

Law stated - 31 July 2026

Electronic invoicing

- 56** | 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?

The US does not currently require private entities to issue invoices electronically, although e-invoices are subject to the same disclosure (including with respect to tax authorities and other agencies), archiving and retention requirements as standard invoices.

Law stated - 31 July 2026

DISPUTE RESOLUTION

Venues

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

Answer in progress.

Law stated - 31 July 2026

ADR

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

Answer in progress.

Law stated - 31 July 2026

UPDATE AND TRENDS

Key trends and developments

- 59** | 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?

Artificial intelligence has emerged as the hottest topic in recent memory, and the White House's January 2025 executive order on 'Removing Barriers to American Leadership in Artificial Intelligence' demonstrated a significant shift in the federal government's approach to the regulation of such advanced technology, as it sought to remove rules and regulations viewed as inhibiting the country's competitive position. Similar to states' enacting privacy

laws in the absence of a comprehensive federal privacy law, states have also begun to enact AI-specific legislation in the absence of a comprehensive federal AI-specific law.

The proliferation of general privacy laws with enhanced data protection obligations has emerged as another trend, but the only general privacy legislation that has been enacted to date in the US has been at the state level. Twenty-three states have enacted such laws since 2018, with 18 of those laws enacted since the start of 2023, and substantial regulatory enforcement has followed in the wake of such state laws. In addition, approximately half of the states that have effective general privacy laws have already enacted amendments to such laws, often to expand protections and enhance obligations with respect to personal data of children and minors, precise geolocation data, and other sensitive data. Also in the data protection area, in recent years there has been an increased regulatory focus on cybersecurity, as both federal and state regulators have been responding to the confluence of rapidly developing technology and rapidly increasing threats. It seems likely that AI, fuelled by massive amounts of data and facilitating cyberattacks at greater scale and more sophistication, will trigger more laws and regulations directed at protecting data and information.

Law stated - 31 July 2026

Linklaters

Ieuan Jolly

ieuan.jolly@linklaters.com

[Linklaters LLP](#)

[Read more from this firm on Lexology](#)