CHAMBERS GLOBAL PRACTICE GUIDES

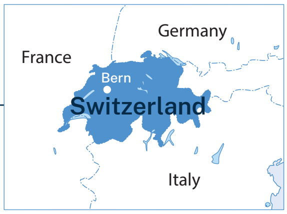
TMT 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Switzerland: Law & Practice

Lukas Morscher, Lukas Staub and Jil Eichenberger
Lenz & Staehelin

SWITZERLAND



Law and Practice

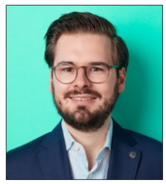
Contributed by:
Lukas Morscher, Lukas Staub and Jil Eichenberger
Lenz & Staehelin

Contents

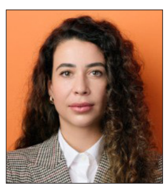
Lenz & Staehelin provides tailored services to clients operating and investing in all areas of the TMT sector, through a dedicated and multidisciplinary TMT team. It advises start-ups, investors, technology companies and established financial institutions in their TMT activities. Drawing on experts in various practice groups for active and cost-efficient advice, when required, the firm strives for long-term trust-based relationships with clients, becoming a partner in the development and marketing of their services throughout their various life cycles. Reflecting the diverse nature of TMT projects, the multidisciplinary team covers the full range of relevant legal services while successfully navigating the regulatory environment through close contact with regulators, including in the areas of banking and finance, TMT and outsourcing, corporate and M&A, commercial and contracts, competition, tax and employment.

Authors

Lukas Morscher is a partner and the head of the technology and outsourcing practice and co-head of the fintech practice in the Zurich office of Lenz & Staehelin, as well as being an expert on digitalisation in the financial services industry. He practises in transactional and regulatory matters, outsourcing (IT and business process transactions), TMT, internet and e-commerce, data privacy, fintech, blockchain and digitalisation. He is a member of SwissICT, Swico, the Swiss-American Chamber of Commerce and the International Technology Law Association (ITechLaw) and is a frequent speaker on topics related to technology and digitalisation.



Lukas Staub of Lenz & Staehelin focuses his practice on technology, regulatory, financial markets and corporate law, as well as data protection, outsourcing and fintech matters. He is a senior associate in the firm's Zurich office and a member of the firm's technology and outsourcing, banking and finance, as well as corporate and M&A practice groups. He frequently advises on all matters around digitalisation and has a deep interest in the application of technology, both within and outside the financial markets. He is a lecturer in compliance at FFHS.



Jil Eichenberger focuses her practice on the fields of data protection, technology, corporate and employment law. She works as an associate in the Zurich office of Lenz & Staehelin, and is a member of the firm's technology and outsourcing, corporate and M&A, intellectual property and employment practice groups. She frequently advises on data protection matters.

Lenz & Staehelin

Brandschenkestrasse 24
CH-8027
Zurich
Switzerland

Tel: +41 58 450 80 00
Fax: +41 58 450 80 01
Email: zurich@lenzstaehelin.com
Web: www.lenzstaehelin.com

1. Digital Economy

1.1 Legal Framework

Under Swiss law, there are no specific regulations for the digital economy, digital services or markets as Swiss legislation is generally technology-neutral. Among the general Swiss laws that apply to the digital economy, the following should be highlighted.

- The Swiss Code of Obligations (the "CO") provides the principles on the conclusion of contracts, including specific customer rights in the case of door-to-door sales which, since 2016, also apply to sales over means of simultaneous communication such as phone calls.
- The Unfair Competition Act (the "UCA") bans certain types of unfair or misleading competitive behaviour and has specific provisions, including on transparency when offering goods or services online, unsolicited marketing over the phone, as well as mass advertising such as through newsletters.
- The Federal Act on Telecommunications (the "TCA") regulates the provision of telecommunications services and also the use of cookies and the principle of net neutrality (see **6. Telecommunications**).
- The Federal Data Protection Act (the "DPA") and its implementing Ordinance (the "DPO") govern the processing of personal data pertaining to individuals (see **2.1 Highly Regulated Industries and Data Protection**).

1.2 Key Challenges

A key challenge for Switzerland's digital economy remains the lack of a broadly accepted, trustworthy framework for electronic identification. Following the acceptance of the Federal Act on Electronic Identity Credentials and Other Electronic Proofs of Identity (the "e-ID Act") in September 2025, the focus has shifted from the legislative process to implementation and market adoption. This notably concerns the roll-out of Switzerland's trust infrastructure and wallet solution ("SWIYU") as well as the availability of interoperable credentials for use in cases in both the public and private sector (see **8. Trust Services and Digital Entities**).

A further key challenge concerns the evolving governance of digital platforms. Switzerland continues to address platform-related issues predominantly through technology-neutral general law (in particular the UCA, personality rights, criminal law and the DPA). However, in addition, the Federal Council has opened a consultation on a draft Federal Act on Communication Platforms and Search Engines, signalling a move towards more specific procedural and transparency obligations for major platforms and search engines (see **10. Social Media**).

1.3 Digital Economy Taxation

In Switzerland, companies and individuals operating in the digital economy and providing digital goods and services are subject to the general tax regime, which includes profit and capital taxes for companies as well as income and wealth taxes for individuals.

Digital services and goods provided to recipients in Switzerland may be subject to Swiss value added tax (VAT) if the relevant requirements outlined in the Swiss VAT Act are met. This implies that non-Swiss providers of these services and goods may have to register for Swiss VAT purposes. Additionally, specific VAT rules for electronic platform providers came into force on 1 January 2025.

With effect from 1 January 2024, Switzerland also implemented Pillar Two of the OECD/G20 Two-Pillar Solution, which will address the tax challenges arising from the digitalisation of the economy. The intention behind Pillar Two is to prevent multinational groups from shifting profits to low-tax jurisdictions through the global introduction of a 15% minimum corporate tax rate for multinational groups with an annual consolidated revenue in excess of EUR750 million.

Managing tax compliance in Switzerland requires a comprehensive understanding of Switzerland's various tax types and decentralised tax system, where federal, cantonal and municipal authorities impose taxes under different regulations and by applying different procedures.

1.4 Taxation of Digital Advertising

No particular rules apply and the general Swiss tax regime is relevant (see **1.3 Digital Economy Taxation**).

1.5 Consumer Protection

Switzerland does not have specific consumer protection laws for digital goods and services. Instead, general rules such as the UCA, liability rules, the Swiss DPA and the CO apply (see **1.1 Legal Framework**).

1.6 The Role of Blockchain in the Digital Economy

Cryptocurrency and distributed ledger technology (DLT), including blockchain, are transforming Switzerland's TMT sector by driving decentralisation, secure transactions and innovative business models. Notable examples include the adoption of cryptocurrency for tax payments by many municipal and cantonal governments, which since 2024, has also included the city of Lugano. The Swiss National Bank's Project Helvetia piloting the Central Bank Digital Currency is also ongoing and UBS's successful piloting of the blockchain-based payment system, UBS Digital Cash, was carried out in November 2024.

The legal challenges presented by cryptocurrency and blockchain technologies in Switzerland include the difficulty of applying traditional legal concepts such as know your customer (KYC) and anti-money laundering (AML) principles in a decentralised and often anonymous environment. These technologies also pose questions around liability, intellectual property and data protection, as they enable rapid and borderless transactions that can be hard to trace and regulate.

On the other hand, the opportunities include the potential for innovation and economic growth, as the Swiss legal framework is generally supportive and flexible, allowing new financial products and services to be developed.

Switzerland's regulatory framework reflects its commitment to fostering blockchain innovation while ensuring regulatory clarity. In 2018, the Swiss Financial Market Supervisory Authority ("FINMA") was one of the first regulatory authorities to publish guidelines on initial coin offerings (ICOs), classifying tokens based on their function and transferability into payment, utility or asset tokens.

In the course of 2021 the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (the "DLT Act") came into force, which amended several federal laws to enhance Switzerland's position as a leading, innovative and sustainable hub for DLT-related activities. Key amendments included the following:

- The Civil Law was amended to increase legal certainty for the transfer of DLT-based securities.
- Changes to the bankruptcy regime provided for the segregation of digital assets in bankruptcy proceedings.
- A new authorisation category of a DLT trading facility, which could offer trading, settlement and clearing services for digital assets, was introduced.

These changes improved market access for fintech companies involved in DLT and blockchain technologies by enhancing legal clarity and reducing regulatory barriers. Further legislation providing for, among others, a specific licensing regime for payment service providers including for issuing stablecoins was proposed by the Swiss Federal Council in late 2025. Such legislation is, however, not expected to come into force before 2028.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

Swiss law does not include specific regulations for cloud or edge computing as it maintains a technology-neutral legislative approach. As such, general legal frameworks, including data protection laws, govern these services.

Personal data must be safeguarded with appropriate technical and organisational measures to prevent unauthorised processing, ensuring data security, availability and integrity, regardless of storage location. Using cloud services may constitute outsourced processing. If cloud servers are located abroad and personal data is not fully encrypted during transfer or storage, this is considered an international data transfer. The Swiss Federal Data Protection and Information Commissioner (the "FDPIC") has issued non-binding guidelines outlining risks and data protection requirements for cloud use.

Professional secrecy obligations, such as banking secrecy (the "Banking Act"), financial institutions secrecy (the "Financial Institutions Act" or "FinIA") and telecommunications secrecy (the "TCA"), apply in addition to the DPA (see **7.1 Legal Framework Challenges**). Sector-specific rules also exist for health-related data processing, including under the Federal Act on Research on Humans, the Federal Act on Human Genetic Testing and the Federal Ordinance on Health Insurance.

Certain cloud service providers may also fall under the Federal Act on the Surveillance of Post and Telecommunications (the "SPTA"), which obliges them to facilitate surveillance measures during criminal investigations when ordered by authorities.

In addition, the Federal Act on Information Security (the "ISecA") and its implementing ordinances entered into force on 1 January 2024. While the ISecA primarily focuses on government cybersecurity, a revision that came into force on 1 April 2025 introduced a mandatory cyber-incident reporting regime for operators of critical infrastructure, including private-sector entities. Hence, qualifying cyber-attacks must be reported to the National Cyber Security Centre (NCSC) within 24 hours of discovery. This obligation applies to Swiss-based providers of cloud services, data centres and certain software or hardware manufacturers as well as banks, insurers and hospitals, among others. Cloud service contracts must clearly address compliance with relevant legal and contractual obligations, particularly data protection requirements imposed on customers of cloud service providers. Sector-specific rules may apply, such as FINMA's Circular 2018/3 (the "Outsourcing Circular"), which applies to most financial institutions subject to supervision by FINMA (see **7. Challenges with Technology Agreements**). Entities supervised by FINMA are also obliged to report cyber-attacks to FINMA in line with FINMA's Guidance 03/2024.

If employee data is processed in the cloud, the specific restrictions under the CO must be adhered to, and Ordinance 3 of the Federal Employment Act limits employers' use of surveillance systems.

Swiss DPA

Switzerland's data protection framework is primarily governed by the revised Federal DPA and the DPO, which both entered into force on 1 September 2023. These laws regulate the processing of "personal data" by private entities and federal bodies, aligning Swiss standards with international norms and addressing technological advancements. Cantonal authorities are subject to separate legislation, and additional federal laws govern data protection in regulated industries, such as financial markets and telecommunications.

The DPA and DPO apply to the processing of any data relating to an identified or identifiable (natural) person. A person is identifiable if a third party, having access to the data on the person, is able to identify that person with reasonable effort. Under the DPA, "sensitive personal data" is considered a special category of personal data that is subject to stricter processing conditions. Sensitive personal data is data on:

- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or affiliation to a race or ethnicity;
- genetic data;
- biometric data that uniquely identifies a natural person;
- administrative and criminal proceedings or sanctions; or
- social security measures.

Furthermore, the DPA provides for stricter processing rules for certain processing activities, including "high-risk profiling" and "automated individual decision-making". "High-risk profiling" refers to any form of automated processing of personal data to use the data to evaluate certain personal aspects relating to a natural person that involves a high risk to the personality or fundamental rights of that natural person, by pairing data that enables an assessment of essential aspects of the personality of the natural person. "Automated individual decision-making" is any decision based exclusively on automated processing of personal data that has a legal consequence for, or a considerable adverse effect on, the data subject.

As a general principle, personal data must always be processed (this includes collection and usage) lawfully. Processing is lawful if it is either processed in compliance with the general principles set out in the DPA (including, among others, the principle that the collection of personal data and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection) or, if non-compliant with these general principles, is justified (eg, by the data subject's voluntary informed consent or by law). The disclosure of personal data to third parties is generally lawful under the same conditions.

Alignment of Swiss Legislation With International Data Protection Standards

The revised DPA closely mirrors the EU General Data Protection Regulation 2016/679 (the "GDPR"), with minor "Swiss finishes". Most notably the sanction system in the DPA targets individuals responsible for breaches/violations directly, whereas under the GDPR, sanctions are imposed on the company itself. This ensures Switzerland maintains its status as a country adequately protecting personal data from an EU perspective, facilitating data transfers. To this effect, the European Commission renewed its adequacy decision for Switzerland in January 2024.

The revised DPA is also aligned with the revised European Convention on Human Rights and Fundamental Freedoms and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (the "Convention ETS 108").

Cross-Border Data Transfers

Personal data may only be transferred outside of Switzerland if adequate measures are in place to ensure that the privacy of the data subject is not significantly at risk, in particular, due to the absence of legislation that guarantees adequate protection in the jurisdiction where the recipient resides. The Federal Council has published a list of jurisdictions that provide adequate data protection in Appendix 1 to the DPO. The EEA countries, Andorra, Argentina, Canada, the Faroe Islands, Gibraltar, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand, the United Kingdom and Uruguay are generally considered to provide an adequate level of data protection as regards personal data, while the laws of all other jurisdictions do not provide adequate data protection.

As regards data transfers to the US, the Swiss-US Privacy Shield (which replaced the US-Swiss Safe Harbour Framework in 2017), under which Swiss companies were able to transfer personal data to their US business partners without the need to procure the consent of each data subject or to put additional measures in place, was declared invalid by the FDPIC in September 2020. Effective 15 September 2024, the Swiss Federal Council approved the adequacy of data protection exclusively for personal data transfers to US companies certified under the data privacy framework (the "DPF"). While this allows data transfers to certified US companies, it does not grant the United States as a whole the status of a country with adequate data protection. Only businesses that meet the certification requirements of the DPF qualify for this facilitated transfer mechanism.

In the absence of legislation that guarantees adequate protection, personal data may only be transferred outside Switzerland if:

- sufficient safeguards (in particular, standard contractual clauses) ensure an adequate level of protection abroad;
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or performance of a contract (and the personal data is that of a contractual party); or
- disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie, binding corporate rules).

In practice, in order to ensure an adequate level of data protection, data transfer agreements or data transfer clauses (ie, binding corporate rules) are regularly used. It is the responsibility of the data transferor to ensure that an agreement sufficiently protecting the rights of the data subjects is concluded. The FDPIC recognises the new set of standard contractual clauses, issued by the European Commission pursuant to the Implementing Decision 2021/914/EU (the "EU SCC"), for data transfers to countries not providing adequate data protection levels, provided the necessary adaptations and amendments are made for use under Swiss data protection law. Since 1 January 2023, data transfers must be based on the EU SCC. This means any previous model contracts to ensure equivalent protection may no longer be used.

Data Protection Officers

The appointment of a data protection officer (DPO) is not mandatory for private controllers. However, by designating a DPO, it becomes possible to consult this DPO instead of the FDPIC in the case of a high-risk processing activity. Release to consult with the FDPIC only applies if the DPO exercises its functions towards the controller in a professionally independent manner and is not bound by any instructions, does not carry out any activities that are incompatible with its tasks and has the required expertise, and the controller publishes the DPO's contact details and notifies the FDPIC thereof.

A reporting portal for contact details of DPOs is publicly accessible on the FDPIC's website. In contrast to private entities, federal bodies are required to designate a DPO. The DPO serves as a contact point for data subjects and for the authorities responsible for data protection in Switzerland. Further tasks include, in particular, training and advising the controller in matters of data protection and providing support on applying the data protection regulations.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

Artificial intelligence (AI) offers new opportunities to develop social or scientific knowledge and can be the basis for further forms of value creation by companies. In general, there is no cross-sector regulation in Switzerland regarding AI. As regards the processing of personal data, the right to privacy and the protection of personal data must be safeguarded (see **2. Cloud and Edge Computing** regarding data protection principles). While government authorities periodically review developments regarding AI, it is currently acknowledged that any regulation should be technology-neutral in order to accommodate new developments within the existing legal and regulatory framework. This enables businesses located in Switzerland to make optimal use of upcoming technologies and advances and to efficiently adapt their business models and processes as required or desired.

The Federal Council has set up a federal working group on AI under the direction of the State Secretariat for Education, Research and Innovation (the "SERI"), which facilitates the exchange of knowledge and opinions and the co-ordination of Switzerland's positions in international bodies. Based on a report submitted by the SERI to the Federal Council outlining existing measures, an assessment of possible fields of action and considerations on the transparent and responsible use of AI, the Federal Council concluded in December 2019 that Switzerland was, in general, well suited to address AI applications, business models and challenges. Therefore, there was no immediate need to adapt the existing legislative framework, subject to certain specific areas (such as mobility, security policy, education and research). However, a multitude of measures were initiated to address corresponding challenges.

In light of recent technological developments, opportunities and challenges associated with AI, the Federal Council instructed the Federal Department of the Environment, Transport, Energy and Communications (the "DETEC") to prepare an overview of possible regulatory approaches to AI. The DETEC published the overview on 12 February 2025. Rather than adopting a general cross-sector AI law, Switzerland will maintain its sector-specific regulatory framework. Additionally, the Federal Council has decided to ratify the Council of Europe's AI Convention and propose the necessary amendments to Swiss law to the Swiss Parliament. A draft is expected by the end of 2026. In line with this approach, overarching regulations governing AI will be restricted to areas concerning fundamental rights, such as data protection. To ensure Switzerland's regulatory approach remains aligned with that of its key trading partners, the Federal Administration will also develop an implementation plan by the end of 2026 for any additional measures not covered by the proposed legislation.

AI in the Federal Administration

With respect to the use of AI in the Federal Administration, the Federal Council has taken a series of steps to establish a legal framework and promote its effective integration. Recognising the potential of AI for improving administrative processes, it adopted guidelines on 25 November 2020 to provide a framework for its application. Building on this, in December 2023, the Competence Network for Artificial Intelligence (the "CNAI") published a fact sheet on generative AI tools. In fulfilment of a mandate by the Federal Council from September 2024, the Federal Chancellery proposed an AI Strategy for the Federal Administration and a corresponding implementation plan on 11 December 2025. The Federal Council subsequently took note of the implementation plan and approved an amendment to the Digitalisation Ordinance. In parallel, the Federal Council also approved a new long-term strategy for its digital business administration (the "GEVER") on 8 January 2025, which is embedded within the broader Digital Federal Administration Strategy, with plans to leverage AI as a supportive tool.

Data Protection

In relation to data protection concerns regarding AI, the FDPIC has issued several pieces of guidance in the last few years. These are as follows.

- Non-binding guidance for AI applications, emphasising that providers of AI applications must inform users in a transparent and comprehensible way of the purpose and means of the processing of personal data (4 April 2023).
- A joint statement with nine other national data protection authorities urging social media platforms and website operators to take measures to protect personal data against data scraping, including for AI model training (24 August 2023).
- A statement pointing out that the DPA is directly applicable to AI-supported processing of personal data (9 November 2023).
- A follow-up statement providing additional guidance on how companies can ensure that the personal information of their users is protected from unlawful scraping (31 October 2024).

Deepfake Technologies

Individuals affected by deepfake technologies can invoke the general protection of personality rights under Article 28 of the Swiss Civil Code, which safeguards against unauthorised infringements of personal identity and reputation. Furthermore, an explicit prohibition of identity theft was introduced in Article 179 of the Swiss Penal Code.

Self-Driving Vehicles

As for self-driving vehicles, the Swiss Federal Council and Parliament have amended the Road Traffic Act and its ordinance to regulate automated vehicles. The new framework came into effect on 1 March 2025 and governs the deployment and operation of self-driving cars in Switzerland.

Drone Regulations

Drone operations in Switzerland are regulated by the Federal Office of Civil Aviation (the "FOCA"). While there are no specific rules for AI in drones, programmed-route drones face stricter requirements than manually operated ones, including mandatory registration and operator training. Since January 2023, the EU Drone Regulation has also applied in Switzerland, introducing standards for drone classification, operator registration and pilot certification to enhance safety and integrate drones into Swiss airspace.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

The internet of things (IoT) refers to objects and devices which are connected to a network such as the internet and which use the network to communicate with each other or make information available. The connecting device may be a modem, network attached storage (NAS), a webcam, intelligent light switches, or smart TVs connected to an internal network or the internet. The Swiss regulatory framework encourages digital services, in particular, due to the technology-neutral approach of the legislation, thereby allowing ample room for development of technology-driven business models and companies.

There are generally no regulation-induced impediments to technological innovation under existing law. Government authorities periodically review developments in technology and generally emphasise the importance of making use of technological progress. Considerable efforts are undertaken to further facilitate market entry for technology-driven business models.

As an increasing number of intelligent devices are connected to the internet, not only has the number of communications participants involved grown, but the number of vulnerable devices that may be misused by hackers (eg, for sending spam emails) has also increased. These devices need to be adequately protected (eg, by using individual passwords or restricted access) and respective software has to be kept updated. Between objects and devices that communicate with each other, large amounts of information and data are typically exchanged.

This may also have an impact on the protection of personal data and the general rules of data protection apply. All data subjects are protected from their personal data either being processed in a way that is not compliant with the law or used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification applies (see **2. Cloud and Edge Computing** regarding key data protection principles).

To protect critical information and communication infrastructure in Switzerland, the Federal Council has created the National Cyber Security Centre (the "NCSC") as an independent federal authority which has been operational since 1 January 2024. To prevent devices within the IoT from being misused by hackers, the NCSC recommends preventative measures on its website. These include:

- the establishment of a separate network segment for devices connected to the internet and devices connected to personal data;
- restricting access from the internet to the device;
- keeping devices up to date and installing updates;
- using protocols allowing only encrypted connection;
- securing access via the internet by means of a VPN connection or restricting access by using an IP address or GeoIP filter; and
- using complex passwords and two-factor authentication.

4.2 Compliance and Governance

Due to the technology-neutral approach of Swiss law, deploying IoT solutions must comply with the general rules of unfair competition law, risks and liabilities and data privacy. In particular, the deployment of IoT devices requires ensuring cybersecurity and data protection, especially given the vast amounts of data, some of it sensitive, generated and shared by connected devices. The NCSC oversees compliance and incident reporting for cybersecurity and, if personal data is involved, the FDPIC will be involved as well (see **2.1 Highly Regulated Industries and Data Protection** and **4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection**). Manufacturers must adhere to conformity regulations under the Federal Office of Communications ("OFCOM") to ensure IoT devices are interoperable and free from interference.

As of 1 January 2025, OFCOM has established two specialised units: the Market Access and Cybersecurity unit, which ensures that wireless devices meet privacy and cybersecurity standards, and the Network and Service Security unit, which focuses on maintaining and enhancing the resilience and availability of telecommunications networks. From 1 August 2025, connected wireless devices, such as smartphones and smartwatches, are required to meet stricter cybersecurity requirements to prevent unauthorised data access, mitigate fraud risks and protect against misuse in cyber-attacks.

4.3 Data Sharing

Switzerland does not have a specific equivalent to the EU's Data Act. Data sharing by IoT companies is governed by general data protection laws (see **2.1 Highly Regulated Industries and Data Protection**). Sensitive data, such as health, biometric or religious information, is subject to stricter protections under the DPA, including enhanced consent requirements. Trade and manufacturing secrets may also raise issues under industrial espionage or competition laws.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Broadcast Media Regulation

The broadcasting sector has three main authorities responsible for the granting of licences. The Federal Council is the licensing authority for the Swiss Broadcasting Corporation (the "SBC"). With respect to other licences, licensing competence has been delegated to the DETEC. OFCOM puts the licences out for tender and consults interested groups. OFCOM further fulfils all sovereign and regulatory tasks related to the telecommunications and broadcasting (radio and television) sectors. It fulfils an advisory and co-ordinating function for the public and policymakers. It also guarantees that basic services are provided in all parts of the country and throughout the population.

The Federal Media Commission (the "FMEC") advises the Federal Council and the Federal Administration in relation to media issues. The Federal Radio and Television Act of 24 March 2006 (the "RTVA"), established an Independent Complaints Authority for Radio and Television, which deals with complaints that relate to the editorial programme and rules on disputes over denied access to a programme. In Switzerland, apart from the communications sector, regulation of the media sector is also dealt with at a federal level. The broadcasting, processing and reception of radio and television programme services are regulated by the RTVA and its implementing ordinances.

Licensing Requirements

Broadcasters of programme services are, in principle, required to obtain a licence. Broadcasters that neither request the splitting of revenue nor guarantee wireless terrestrial distribution may operate their service without a licence. However, these broadcasters need to notify OFCOM. Broadcasters of programme services of minor editorial importance (such as programme services that can only be received by fewer than 1,000 people at the same time) do not fall under the scope of the RTVA and do not need a licence or registration. If the broadcaster of a radio programme service is granted a licence under the RTVA, it is at the same time granted a licence under the TCA for use of the frequency spectrum. This means no separate application is needed. Cable TV operators are under a duty to broadcast, in the respective coverage area, the TV programme services of broadcasters that have been granted a licence. Licences are awarded by public tender.

To be awarded a licence, the applicant must:

- be able to fulfil the mandate;
- possess sound financial standing;
- be transparent regarding its owners;
- guarantee compliance with employment law regulations and the working conditions of the industry, the applicable law and in particular, the obligations and conditions associated with the licence;
- maintain a separation of editorial and economic activity; and
- have registered offices in Switzerland.

In general, the number of licences a broadcaster and its group companies may acquire is limited to a maximum of two television and two radio licences (this does not apply to the SBC). If there are several applicants for one licence, preference will be given to the candidate that best fulfils the performance mandate. Often, independent applicants (ie, those not belonging to a media corporation that already possesses other licences) are deemed to be better able to fulfil this criterion by the DETEC. The fee per year for a broadcasting licence amounts to 0.5% of the gross advertising revenue that exceeds CHF500,000, and administrative charges will be incurred in relation to the radio and TV licence as well as to the telecommunications licence, calculated on the basis of time spent. A reduced rate applies to the granting, amending or cancelling of a licence for the broadcasting of a radio or television programme service as well as for the radio communications licence.

There are no rules specifically applicable to the operation of online video channels (such as YouTube) or on-demand streaming platforms (such as Spotify or Netflix). As these platforms provide on-demand rather than linear services, they are not subject to licensing under the RTVA. Since Swiss legislation strives to keep laws technology-neutral, the general rules apply to the operation of online video channels.

Quota and Investment Obligation in Swiss Film Production

On 15 May 2022, a quota and an investment obligation in Swiss film production for streaming services was approved in a public vote. The approval led to an amendment to the Film Act of 14 December 2001 (the "FiA") requiring the implementation of provisions regarding a European quota and an obligation to invest in Swiss film-making through the Ordinance on the Quota for European Films and Investment in Swiss Film Production (the "FQIO"). The provisions came into force on 1 January 2024 and included the following obligations:

- streaming service providers must invest 4% of the revenue generated in Switzerland into Swiss film productions;
- the investment may be made either directly in Swiss film production or by payment of a substitute levy which will be used to support Swiss film production; and
- at least 30% of the series or films streaming service providers broadcast must be produced in Europe.

In October 2023, the Federal Office of Culture issued practical guidance on the quota and investment obligation on its website.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

In Switzerland, the telecommunications sector is regulated at a federal level by the TCA as the primary legal framework. The TCA governs the transmission of information via telecommunications techniques, excluding television and radio programme services. Key supplementary laws include:

- the Federal Ordinance on Telecommunications Services of 9 March 2007 (the "OTS"); and
- the Federal Ordinance on Telecommunications Installations of 25 November 2015 (the "TIO"), ensuring alignment with international and European standards for electronic communications equipment.

The Federal Council issues technical regulations for telecommunications installations, including requirements for conformity assessment, certification and basic technical specifications, while OFCOM designates technical standards to ensure compliance. The telecommunications legal framework applies to telecommunications service providers (TSPs), which are providers of services qualifying as telecommunications services. The TCA defines TSPs as services transmitting information for third parties using telecommunication techniques, which include the sending or receiving of information by wire, cable or radio using electrical, magnetic, optical or other electromagnetic signals.

ComCom and OFCOM

Switzerland's telecommunications sector is regulated by two agencies, the Federal Communications Commission (the "ComCom") and OFCOM. Fixed-line, mobile telephony and satellite services fall under the TCA and its implementing ordinances. Under a revision, which came into effect on 1 January 2021, consumer protection was enhanced (eg, international roaming, open internet and safeguarding minors) while promoting deregulation and administrative simplification, such as abolishing general notification and licensing requirements. Among other things, the registration obligation for TSPs has been limited to TSPs which, for the provision of telecommunications services, use:

- radio frequencies that require a licence; or
- resources administered on a national level (eg, short numbers that are assigned to emergency calls or rescue and breakdown services).

All other TSPs remain subject to the TCA obligations but are no longer required to register with OFCOM. The ComCom grants universal service licences to ensure nationwide access to essential telecommunications services.

VoIP Service Providers

Providers of Voice over Internet Protocol (VoIP) services are not regulated under the TCA if they solely offer online services without transmitting data using telecommunications techniques. However, if a VoIP provider qualifies as a TSP (eg, when a customer can be reached via a fixed-line number within the public switched telephone network), the TCA applies. Even in these cases, the ComCom does not impose all of the TCA obligations on these providers. For example, they are not required to offer free carrier pre-selection (as no direct link exists between a network and a service operator) or to provide caller location information for emergency calls (due to technical limitations).

In Switzerland, telecommunications providers must adhere to general data protection laws as well as the specific security obligations set out in the TCA and its implementing ordinances. These require providers to ensure the security of data processing and transmission, uphold strict confidentiality for subscriber communications and related data, and prevent unauthorised manipulation of telecommunications systems. To protect infrastructure and minimise risks, providers may implement measures such as rerouting or blocking connections.

6.2 Net Neutrality Regulations

Net neutrality refers to the principle that all internet data traffic should be treated equally, without discrimination or preference. Internet access providers must remain impartial toward applications, services, content and connected devices.

Net neutrality was codified in the revised TCA, which came into effect on 1 January 2021. The corresponding ordinance prohibits TSPs from unjustifiably blocking, throttling or prioritising third-party services, ensuring consumers can freely access their preferred internet services, applications and content.

6.3 Emerging Technologies

Switzerland's technology-neutral legislation ensures that general rules on risks, liabilities and data protection apply broadly to emerging technologies like 5G, IoT and AI (see **3. Artificial Intelligence** and **4. Internet of Things**). However, Switzerland has acknowledged that emerging technologies may require targeted regulatory updates to address specific challenges. For example, the Federal Council has highlighted cybersecurity and geopolitical risks linked to 5G networks inspired by the EU's 5G toolbox. As an initial regulatory step, on 14 January 2026 the Federal Council adopted a partial revision of the OTS, entering into force on 1 March 2026, requiring mobile network operators to ensure an emergency power supply at key sites from 2031 and introducing further service continuity requirements from 2034. In addition, the Federal Council is expected to propose amendments to the TCA to parliament in the second half of 2026 focusing on the security of critical infrastructures and provisions enabling action should geopolitical risks materialise.

7. Challenges With Technology Agreements

7.1 Legal Framework Challenges

Swiss law does not specifically regulate IT service agreements but governs general outsourcing to IT providers in certain industries, such as finance, telecommunications and the public sector. With regards to financial services, the sector-specific regulation set out below applies to the outsourcing of business areas (infrastructure or business processes).

Professional Secrecy and Banking Secrecy

The various professional secrecies applicable to certain Swiss industries such as lawyers, auditors, banks and other financial institutions prohibit the disclosure of client-identifying data (CID) to third parties whether within or outside Switzerland, subject to criminal sanctions up to imprisonment. CID may therefore only be shared with third parties (eg, suppliers) as provided by law or if the relevant customers have provided consent. In the absence of an established court practice, the highest certainty would need to be provided by specific and separate prior written consent. Institutions such as banks are increasingly relying on consent provided for in their general terms of business. Market practice based on some recent views (which were also published through the Swiss Bankers Association) increasingly take the position that an individual waiver is not required for disclosing CID to a service provider (even abroad) in case of sufficient contractual guarantees and appropriate technical and organisational measures.

Professional secrecies do not restrict transferring encrypted or fully anonymised data (where the recipient cannot identify individual customers).

The FINMA "Outsourcing Circular"

FINMA's "Outsourcing Circular" in essence covers all institutions supervised by FINMA including banks, insurers, managers of collective assets, fund managers and self-managed *sociétés d'investissement à capital variable* ("SICAVs") and branches of equivalent foreign financial institutions.

Before outsourcing significant business areas, these institutions must comply with the detailed measures set out in the "Outsourcing Circular", including the following.

- The obligation to keep an inventory of all outsourced services, which must include:
  (a) proper descriptions of the outsourced function;
  (b) the name of the service provider and any subcontractors; and
  (c) the service recipient and the person or department responsible within the company.
- Careful selection, instruction and control of the supplier.
- Conclusion of a written contract or a contract in some other format that can be evidenced in text form with the supplier setting out, among other things, the services to be provided, security and business continuity requirements as well as audit and inspection rights.

The customer remains responsible for overseeing outsourced business areas. Swiss banks, securities firms and insurers must also account for the increased operational risks associated with outsourcing to independent service providers, which can result in additional capital requirements.

Essential Service Outsourcing

A financial market infrastructure subject to the Financial Market Infrastructure Act (the "FMIA") and the implementing ordinance (the "FMIO") (which includes a stock exchange, multilateral trading facility, central counterparty, central securities depository, trade repository or payment system), requires approval from FINMA to outsource essential services like risk management. If such outsourcing is proposed by a financial market infrastructure that the Swiss National Bank (SNB) considers to be systemically important, FINMA must consult with the SNB beforehand.

When outsourcing an essential service, the financial market infrastructure must:

- carefully select, instruct and control the service provider;
- integrate the outsourced service into its internal control system; and
- monitor the services rendered by the service provider on an ongoing basis.

Reciprocal rights and duties must be set out in a written agreement with the service provider. The financial market infrastructure remains responsible for complying with its obligations under the FMIA. Cross-border outsourcing requires measures to safeguard professional confidentiality and data protection and affected parties must be informed if their data is transferred abroad. The infrastructure, its internal and external auditors, FINMA, and (if systemically important) the SNB must be able to inspect and review the outsourced service.

Requirements of Financial Institutions

Under the FinIA and its implementing ordinance (the "FinIO"), financial institutions (ie, portfolio managers and trustees not subject to the "Outsourcing Circular" as well as managers of collective assets, fund managers and securities firms which are subject to the "Outsourcing Circular") may only delegate tasks to third parties with the necessary skills, experience and authorisation. They must also properly instruct and supervise these third parties. FINMA may require that delegating investment decisions to a foreign third party be subject to a co-operation and information exchange agreement with the relevant foreign supervisory authority, especially if mandated by that country's laws. If a financial institution outsources significant functions, the service provider is subject to information, reporting and audit obligations by FINMA.

The liability of financial institutions and their corporate bodies is governed by the CO. If a financial institution outsources a task, it remains liable for any damages caused by the service provider unless it can prove that it exercised due diligence in selecting, instructing and monitoring the provider (special rules may apply to fund managers).

Requirements of Financial Services

Under the Financial Services Act, financial services providers (including client advisers and providers of financial instruments, ie, much wider than supervised financial institutions) may only delegate tasks to third parties with the necessary skills, experience and authorisation. They must carefully instruct and supervise these third parties. If a secondary (subcontracted) financial services provider performs financial services for the principal's clients, the principal remains liable for:

- the completeness and accuracy of the client information;
- fulfilling the duties in relation to the information;
- the adequacy and suitability of the financial services; and
- documentation and accountability.

If a secondary financial services provider reasonably suspects that client information is incorrect or the principal has not fulfilled its duties, it may provide its service only after it has ensured the completeness and accuracy of the information and ensured compliance with the code of conduct.

Personal Data Protection

The outsourcing of services to an IT service provider may also impact the protection of personal data. Any data subject is protected from their personal data being processed in a way that is not compliant with the law or being used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification applies (see **2. Cloud and Edge Computing** regarding data protection principles).

However, personal data may be given to outsourcing suppliers based on a contract or statutory law if the customer ensures that:

- the supplier will only process data in a way that the customer is itself entitled to;
- the supplier will comply with the applicable data security standards; and
- there are no statutory or contractual secrecy obligations prohibiting this data processing.

Given the customer's liability for the supplier's compliance with data protection laws and the growing importance of data security, liability caps are often excluded in outsourcing agreements, especially for breaches involving sensitive data like business secrets or bank customer information.

7.2 Service Agreements and Interconnection Agreements

Telecommunications Service Agreements

Telecommunications service agreements are not conclusively codified in Swiss law. The TCA defines telecommunications services as transmission of information for third parties by means of telecommunications techniques. Additionally, network infrastructure is a core element of these agreements, which the TCA defines as devices, lines or facilities intended for or used in the technical transmission of information.

In principle, telecommunications service agreements are divided into two segments:

- the upstream market (between providers, focusing on infrastructure and services); and
- the downstream market (between providers and consumers, offering self-procured or purchased services).

Due to their complexity and need for adaptability, these agreements are typically structured into a main contract, service level agreements (SLAs), service definitions and general terms and conditions. To prevent contradictions, subcontracts are arranged hierarchically.

Interconnection Agreements

The TCA defines interconnection agreements as contracts that connect the installations and services of two telecommunications providers, enabling logical and technical interoperability and access to third-party services. The goal is to maximise connectivity by integrating different networks.

Accordingly, the TCA imposes contracting obligations on TSPs providing basic services and market-dominant TSPs, requiring them to offer interconnection in a non-discriminatory, transparent and cost-based way. If access conditions are not agreed upon within three months, the ComCom will decide based on OFCOM's proposal at the request of either party.

While parties are generally free to determine contract terms, the TCA mandates that agreements be in writing and include key elements such as general commercial conditions, service descriptions, technical specifications and implementation terms. For agreements with market-dominant providers, fees must adhere to principles of non-discrimination, cost orientation and transparency.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The CO sets out the principles governing e-signatures and refers to the Electronic Signatures Act (the "ESA") for the technical details, which in turn refers to its respective ordinance. An e-signature is defined as electronic data that is joined or linked logically to other electronic data and which serves to authenticate the other data.

The ESA distinguishes four levels of e-signatures:

- regular e-signatures;
- advanced e-signatures;
- regulated e-signatures; and
- authenticated e-signatures.

The authenticated e-signature, in combination with an authenticated time stamp, is deemed equivalent to a handwritten signature. While regulated e-signatures are not deemed equivalent to handwritten signatures, they may be used, for example, to evidence the authenticity of electronic invoices or to guarantee the integrity of electronically archived documents. Both authenticated and regulated e-signatures can only be obtained from a recognised provider of certification services. A list of all the providers in Switzerland is available on the competent federal authority's website.

Authenticated e-signatures are treated like handwritten signatures. Therefore, e-signatures cannot be used where the law sets out additional formal requirements, for example, in the case of a will (which must be handwritten in its entirety) or real estate deals (requiring a public deed). Additionally, authenticated and regulated e-signatures are only available for natural persons, not for legal entities. However, natural persons can sign electronically on behalf of a legal entity using their personal authenticated e-signature. In addition, entities in possession of a unique business identification number may obtain a regulated electronic seal, which is essentially equivalent to a regulated e-signature.

Although e-signatures were introduced more than ten years ago, their use in Switzerland is limited. To date, only a small percentage of the population has an e-signature. This may be explained by Swiss law's freedom of form, enabling parties to contract without formal requirements in most cases, as well as the relatively high cost and complicated application of e-signatures and the prepayment policy applied by many online businesses, shifting the risk to the customer, who needs to trust that the other party will indeed fulfil its contractual obligations. Since payment has already been received, online businesses generally do not need to verify the customer's identity.

Electronic Identification

After the rejection of a first proposal for an act governing electronic identification services in a popular vote in 2021, the Federal Council finalised a new draft bill and submitted it to parliament for consideration in 2023. The new e-ID Act was approved by the electorate in a popular vote on 28 September 2025. It foresees, among other things, that:

- the federal government will provide an app for smartphones in which the e-ID can be securely managed;
- the federal government will be responsible for issuing the e-ID and will operate the infrastructure serving as a basis for the e-ID;
- users will have the most control possible over their data (self-sovereign identity) and data protection will be ensured, among other things, by the system itself (privacy by design) and by minimising the required data flows (principle of data minimisation) as well as by decentralised data storage;

- the Swiss e-ID system will meet international standards so that it may also be recognised and used abroad in the future;
- the use of an e-ID will be voluntary and free of charge; and
- all authorities, including cantons and municipalities, will be obliged to accept the e-ID when they conduct an electronic identification (eg, when issuing a confirmation of residency or an extract from the debt enforcement register).

The government infrastructure to be created for the purpose of the e-ID will also be made available for use by municipal and cantonal authorities as well as private parties. The Federal Council plans to offer the e-ID as of 2026. Switzerland's new e-ID, "SWIYU", will be implemented in two stages. In the first stage, a secure trust infrastructure will be established. In the second stage, privacy protections will be enhanced.

9. Gaming Industry

9.1 Regulations

In Switzerland, gaming is regulated through general laws and the new Federal Act on the Protection of Minors in respect of Films and Video Games (the "YPA"), which came into effect on 1 January 2025. The YPA introduced content and age restrictions for video games, aiming to protect minors from harmful content, ensuring uniform labelling and control across the country. Game developers and providers share responsibility for this protection.

The Swiss Gambling Act (SGA) which came into effect on 1 January 2019 governs games with gambling elements, requiring developers or publishers to obtain a licence for these games. This requirement only applies to games and players in Switzerland. Loot boxes have been a subject of concern, but the Swiss Federal Gaming Board (the "ESBK") has not definitively classified them as gambling. As of January 2025, the ESBK maintains that loot boxes are a minor part of the gaming experience and not primarily a game of chance. Enforcement against international companies is challenging and without substantial complaints, the ESBK is unlikely to alter its stance.

Key legal challenges include enforcing age and content restrictions, regulating gambling elements and addressing the potential addictive nature of loot boxes. Legislative amendments may be necessary to close enforcement gaps and introduce stricter penalties for non-compliance.

9.2 Regulatory Bodies

Switzerland does not have a specific regulatory authority dedicated exclusively to overseeing the gaming industry. However, certain bodies do have oversight responsibilities depending on the nature of the game.

The Federal Social Insurance Office (FSIO) and the Federal Council oversee the compliance of the relevant cantonal authorities with age restrictions for video games and other media, ensuring the legal requirements are met. The YPA grants them the authority to revoke age classifications if the standards are deemed inadequate.

In Switzerland, gambling games are categorised into three categories:

- casino games;
- major games; and
- minor games.

Casino games are available in both physical casinos and online, and include roulette, blackjack, poker, punto banco and slot machines. Offering these games requires a casino concession from the Federal Council and an operating permit from the ESBK, which also oversees casinos.

Major games, which are also offered online, encompass lotteries, sports betting and games of skill and are licensed and supervised by the intercantonal gambling supervisory authority (the "Gespa").

Minor games, which are not available online, include small poker tournaments, local sports betting and small lotteries and are regulated by cantonal authorities.

The ESBK or the Gespa can block access to websites offering illegal online gambling. Violations of the SGA can result in penalties of up to three years' imprisonment or fines for felonies and misdemeanours, and fines of up to CHF500,000 for contraventions.

9.3 Intellectual Property

Under Swiss law, video games are protected as audiovisual works and/or software works under copyright law. If intellectual property rights, such as copyrights or trade marks, are infringed (eg, unauthorised use of a work or a trade mark within a game), remedies under Swiss law include cease and desist orders, damages or actions to stop further infringement.

The Federal Supreme Court addressed the issue of sale and distribution of video games in 1998, notably in the *Nintendo case*, where it established the principle of international exhaustion of copyright. Therefore, importing and selling video games in Switzerland, after lawful release abroad with the copyright holder's consent, does not infringe copyright. This principle was reaffirmed in a later case in 2007, emphasising that video games are not subject to the national exhaustion exception of certain audiovisual works.

Additionally, user-generated content in video games is protected by IP law in Switzerland, provided it meets the originality and creativity thresholds required for copyright protection. Overall, Switzerland's IP framework supports a broad and technology-neutral application of copyright and trade mark law, ensuring robust protections for various aspects of the gaming industry.

Copyright for Virtual Goods and Assets

Establishing copyright protection for virtual goods in games is challenging. Swiss law requires works to be the result of personal intellectual creation with individual character. Virtual items generated through gameplay or automated processes, such as those earned in-game, will in most cases not meet this threshold, as they lack the necessary originality.

Trade Marks for Virtual Goods and Assets

On 1 January 2024, the Swiss Federal Institute of Intellectual Property (IIP) published updated guidelines addressing trade marks for virtual goods, assets and non-fungible tokens. These guidelines define virtual goods as non-physical items used in virtual environments and classify them under Class 9, like other downloadable digital goods. For trade mark applications, it must be specified that virtual goods are "downloadable" and described with the same precision required for physical goods. Additionally, the updated guidelines incorporate the new rule from Section 4.2, Part 2, of the General Remarks of the Nice Classification regarding services provided in virtual environments.

The method of delivering a service, virtually or physically, generally does not affect its classification. However, if the delivery method affects the service's purpose or result, this distinction becomes relevant. For example, transportation services in Class 39, catering services in Class 43 and material processing in Class 40 serve different purposes in virtual environments and must be classified accordingly using terms like "simulated", "in a virtual environment" or "for entertainment purposes".

10. Social Media

10.1 Laws and Regulations for Social Media

Switzerland lacks specific legislation regulating social media platforms, instead applying general legal principles such as data protection laws and personality rights under the Swiss Civil Code (see also **3.1 Liability, Data Protection, IP and Fundamental Rights**). In particular, there are no age restrictions for social media use, nor specific rules governing data monetisation. However, data monetisation is permissible within the framework of lawful data processing under existing laws.

In recent years, experts in Switzerland have raised concerns related to social media platforms, including concerns over the lack of transparency in algorithms, as well as the spread of hate speech, false information and conspiracy theories. These issues highlight the growing need for oversight of social media platforms.

Although the Federal Council initially deemed social media-specific regulation unnecessary in 2017, its stance evolved in 2023 following international developments like the European Digital Services Act. OFCOM was tasked with drafting a proposal for regulation aimed at ensuring transparency and accountability in algorithmic recommendations, implementing user-friendly reporting and complaint mechanisms, and introducing enforcement measures with sanctions for non-compliance. Although the proposal was initially expected by the end of 2024, its completion has been delayed and remains pending.

10.2 Regulatory and Compliance Issues

Switzerland does not have a dedicated authority exclusively overseeing social media platforms. However, the FDPIC ensures compliance with Swiss data protection laws in the digital sphere, including social media, and provides guidance and recommends measures to address violations and conducts investigations. It has issued recommendations emphasising transparency and user consent for handling personal data on social media. The courts also play a role in enforcing individual rights under data protection and civil law, addressing issues such as defamation, privacy breaches and unauthorised use of personal data.

Recent enforcement actions illustrate the legal framework's reach. In 2020, the Federal Supreme Court ruled that users could be held criminally liable for sharing or liking defamatory or hateful content on social media. In September 2024, the Zurich Commercial Court rejected FIFA's claim against Google for alleged personality rights violations, ruling that the offending content only appeared in search results when users entered specific terms, linking the issue to user behaviour rather than Google's indexing practices.

11. Data Privacy and Cybersecurity

11.1 Data Privacy in Telecommunications

In Switzerland, TSPs must comply with the DPA and DPO (see **2.1 Highly Regulated Industries and Data Protection**) as well as sector-specific confidentiality and security duties under the TCA and its implementing ordinances (see **6. Telecommunications**).

Telecommunications secrecy is a core privacy guarantee founded in the Federal Constitution and reinforced by criminal law. Under Article 321ter of the Swiss Criminal Code (SCC), any unlawful disclosure to a third party of customers' post, payments or telecommunications is subject to a custodial sentence of up to three years or to a monetary penalty. However, statutory co-operation and lawful surveillance remain reserved, in particular, to the surveillance regime under the SPTA and the exemption for official surveillance carried out under express legal powers subject to court approval (Article 179octies of the SCC). Accordingly, TSPs must reconcile telecommunications secrecy with co-operation and data-retention duties under the SPTA and its implementing ordinances. Depending on their statutory classification, these duties may, in addition to TSPs, also extend to providers of derived communication services (ie, services based on telecommunications services enabling one-way or multi-party communications). Upon a lawful order, such duties include providing the required data and assistance and retaining specified secondary telecommunications data (traffic metadata) for six months.

Where TSPs operate websites/apps, the TCA's end-device rule for cookies and similar technologies requires that users are informed and can refuse non-essential technologies. Recent guidance by the FDPIC ("Cookie Guidelines") further raises practical expectations on rejection options and default settings.

Cross-border data transfers are permissible under the DPA subject to the international transfer regime. Switzerland does not impose a general data localisation requirement for telecoms customer data. However, outsourcing and cloud set-ups must be structured so that telecommunications secrecy, data security and auditability are maintained, and appropriate safeguards are in place where the recipient jurisdiction is not deemed adequate under data protection laws (see "Cross-Border Data Transfers" under **2.1 Highly Regulated Industries and Data Protection**).

From a compliance perspective, telecommunications customer-data governance is driven by the operational need to process traffic data and, where relevant, location data for service provision, billing, fraud prevention and network integrity (see **6. Telecommunications**). Compliance is therefore implemented primarily through strict purpose limitation and access controls within the legal and regulatory framework.

11.2 Cybersecurity in Digital Media and Streaming Services

The primary legal and operational challenges for digital media and streaming providers in Switzerland lie, firstly, in ensuring an appropriate level of data security across the service (confidentiality, integrity and availability), in particular for account and payment/subscription environments and against unauthorised access, data leakage and service disruption. Secondly, providers must retain effective oversight over the processing of usage and preference data for personalisation, measurement and advertising purposes and ensure that transparency as well as consent and refusal/withdrawal for non-essential tracking are implemented in the underlying data flows and also enforced against integrated third parties. Thirdly, providers must maintain incident readiness (in particular, timely detection, containment and clarification) so that any notifications (in particular, to the FDPIC) and, where required, information for data subjects can be made without undue delay.

Privacy-by-design/default and security-by-design under Swiss law must be embedded in platform governance and architecture. This typically includes data minimisation by default, strict purpose binding, granular role-based access and segregation, encryption and key management commensurate with risk, controlled logging, and secure development and change management. For high-risk processing (eg, certain profiling constellations), a DPIA under the DPA is typically required in order to assess and document the relevant risks and the measures implemented to mitigate them (see **2.1 Highly Regulated Industries and Data Protection**).

Third-party integrations must be structured so that effective oversight, data security and transparency remain ensured, notwithstanding external dependencies. This requires clear role allocation (controller v processor), enforceable contractual and technical safeguards and, where relevant, compliance with the cross-border transfer regime (see "Cross-Border Data Transfers" under **2.1 Highly Regulated Industries and Data Protection**).

Emerging Swiss cybersecurity obligations primarily affect operations and technology agreements through incident co-operation and reporting readiness. Where a provider (or a critical supplier in its delivery chain) is subject to the statutory reporting duty for cyber-attacks on critical infrastructure, cyber-attacks must be reported to the NCSC within 24 hours (see **2.1 Highly Regulated Industries and Data Protection**).

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com