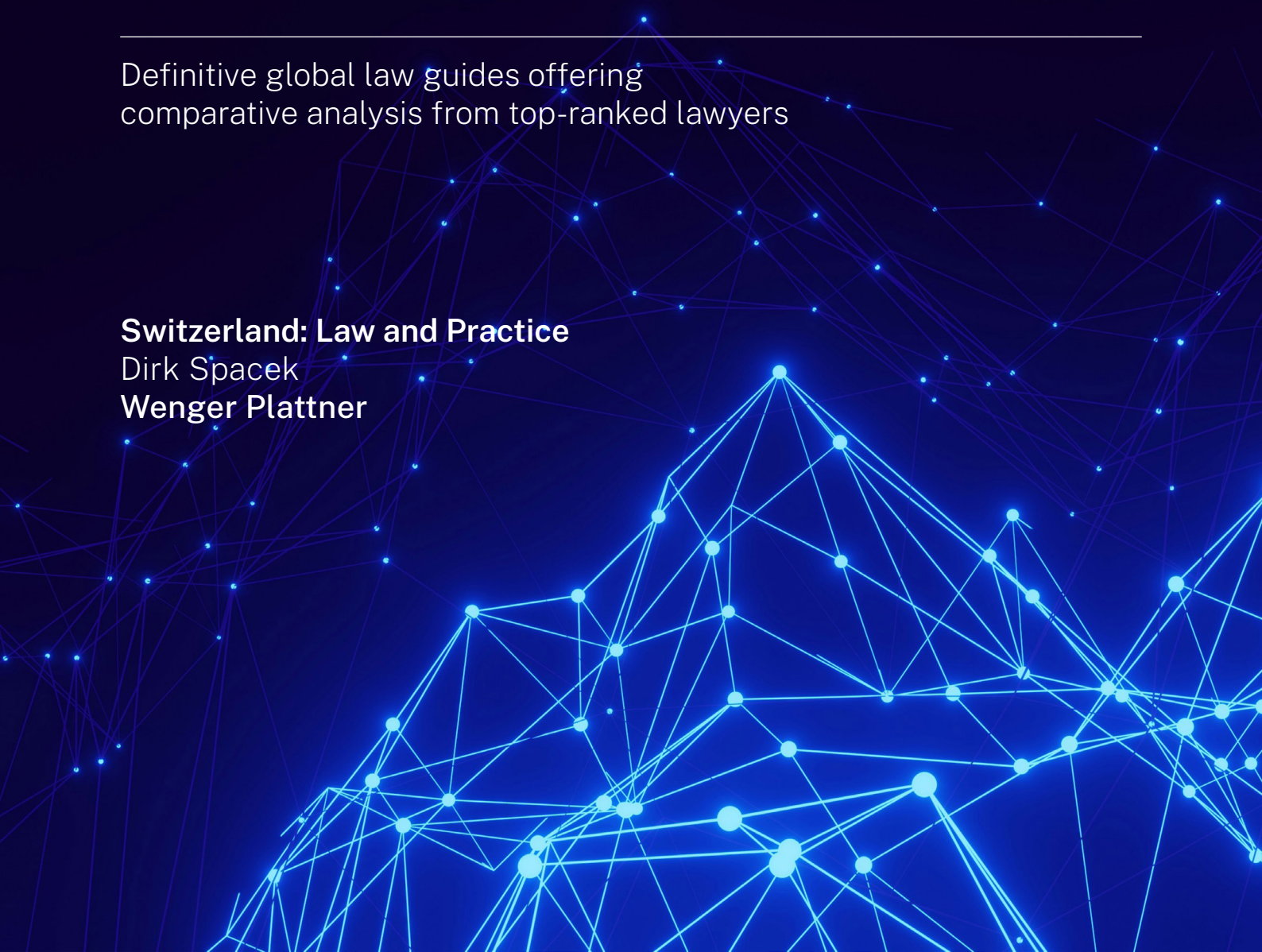
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

# Information Technology 2026

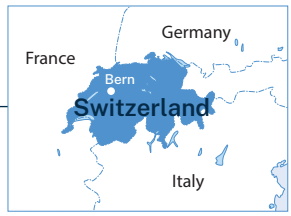
Definitive global law guides offering comparative analysis from top-ranked lawyers



**Switzerland: Law and Practice**

Dirk Spacek
**Wenger Plattner**

# SWITZERLAND



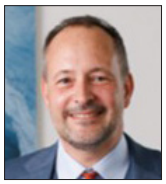

## Law and Practice

**Contributed by:**
Dirk Spacek
**Wenger Plattner**

## Contents

**Wenger Plattner** has been advising and representing clients in all areas of business law for over 40 years. The firm has more than 100 employees at three locations: Basel, Zurich and Berne. Wenger Plattner is a fully integrated partnership. Concerns are handled with high quality and efficiency by the expert who has the necessary expertise and experience for the case. Wenger Plattner develops easily implementable solution concepts and support measures with optimal economic results.

## Author



**Dirk Spacek** is a partner at Wenger Plattner specialising in technology, intellectual property, commercial matters and digital media, with a particular focus on data-driven business models and regulatory matters. His expertise covers intellectual property (structuring and enforcing IP portfolios), regulation of online platforms, digital media, entertainment, e-commerce, IT, data protection and matters related to cybersecurity and cyber crime. He regularly represents clients in complex contract disputes and is also a recognised mediator with the ITDR (Institution for IT and Data Dispute Resolution).

### Wenger Plattner

Seestrasse 39
8700 Küsnacht
Switzerland

Tel: +41 0432 223 800
Email: dirk.spacek@wenger-plattner.ch
Web: www.wenger-plattner.ch

Wenger Plattner

# 1. Online Services and Products

## 1.1 Online Harms or Digital Services Legislation

### 1.1.1 Key Obligations for Online Services

Switzerland does not yet have a comprehensive, dedicated law equivalent to the EU Digital Services Act. Obligations for online service providers to avoid online harm are primarily derived from the Swiss Criminal Code (CC, SR 311.0), the Swiss Civil Code (SCC, SR 210), the Swiss Federal Act on Data Protection (FADP, SR 235.1), and sectoral statutes like, eg, the Swiss Telecommunications Act (TCA, SR 784.10).

Key obligations in these statutes may include the following.

- Content moderation and removal – providers must prevent or remove criminal content, eg, hate speech, child sexual abuse material, or criminal threats as well as personality-infringing content (CC, Articles 135–197 and SCC, Article 28 et seq). Voluntary measures are emphasised, guided by the Federal Council's recommendations on online moderation.
- Transparency – clear terms of service and information on moderation policies must be provided to users (FADP, Articles 13–15).
- Data protection and security – adequate technical and organisational measures to safeguard personal data are required (FADP, Articles 7–10) as a lack thereof could expose individuals to harm.
- Co-operation with authorities – providers must reasonably assist law enforcement in investigations and preserve relevant data when requested (CC, Article 302 et seq).

While there is no specific Swiss "digital services act", the Federal Council has signalled that future Swiss legislation generally aims to align with international standards.

### 1.1.2 Categories of Platforms

Switzerland's laws do not categorise platforms like under the EU Digital Services Act. Obligations under the legal statutes mentioned in **1.1.1 Key Obligations for Online Services** apply in general, regardless of platform size or type. However, distinctions may arise from practice or guidance.

- Telecommunications vs other online services – providers of public communication networks (TCA) face stricter obligations regarding data security, traffic monitoring, data retention, and co-operation with authorities (eg, under the Federal Act on Surveillance of the Swiss Post and Telecommunications Traffic, FAST, SR 780.1). Certain types of online service providers can sometimes qualify as "providers of derived communication services" (eg, cloud or OTT (Over-The-Top) service providers) and may therefore be subject to increased data retention and co-operation duties with authorities under the FAST.
- User-generated content platforms – voluntary content moderation recommendations from the Federal Council emphasise platforms hosting significant user content, particularly large-scale social networks, to implement more robust measures against illegal content. It is worth mentioning that so far, Swiss case law has only confirmed contributory civil liability for personality-infringing content to hosting providers (BGE 139 III 209) whereas it has denied such liability for online copyright violations to access providers (BGE 145 III 72).
- Commercial vs non-commercial platforms – commercial providers must comply with stricter transparency, privacy and liability expectations, while private or small-scale platforms face fewer regulatory pressures.

Swiss regulation currently focuses on the nature of content and service function rather than rigid legal categorisation by size or reach. Future legislation may introduce such distinctions over time.

### 1.1.3 Relevant Regulators and Enforcement

Switzerland does not have one single dedicated regulator for online content or digital services, unlike the EU's Digital Services framework. Enforcement is scattered across authorities depending on the type of obligation at stake.

- Federal Data Protection and Information Commissioner (FDPIC) – oversees compliance with the FADP. Powers include conducting investigations,

issuing binding recommendations and imposing administrative measures; the new FADP (effective 2023) allows for criminal sanctions for serious breaches against individuals in charge of data processing.
- The Cantonal and Federal Law Enforcement Authorities enforce the CC (Criminal Code) regarding illegal online content. Powers include ordering content removal, seizing data, and prosecuting of criminal offences.
- The Federal Office of Communications (OFCOM) supervises compliance for telecommunication and public communication platforms under the TCA. It can issue warnings, enforce technical requirements and impose administrative fines.

Switzerland's approach relies on different existing sectoral regulators rather than a centralised digital services authority, and no EU-style Digital Services Co-ordinator designation exists. Investigative powers are reactive and case-specific.

## 1.2 E-Commerce

### 1.2.1 Principal E-Commerce Legislation

In Switzerland, e-commerce and online contracting are primarily governed by the Swiss Code of Obligations (CO, SR 220), which sets out general rules on contracts, offer and acceptance, and electronic signatures (Articles 1–40, CO for general contract formation; Article 14, CO allows electronic signatures, unless a written signature is required by law). The CO also covers provisions on codified types of contracts (eg, sales contracts, service agreements or work agreements) which may also apply in e-commerce, depending on the contract at stake.

Complementary legislation includes:

- Federal Act on Electronic Signatures (ESigA, SR 943.03) – recognises qualified electronic signatures as legally equivalent to handwritten signatures, enabling secure online contracting;
- FADP – regulates the collection, processing, and storage of personal data during e-commerce transactions;
- Federal Act against Unfair Competition (FAUC, SR 241) – applies to misleading advertising and online commercial practices; and
- sectoral rules – eg, TCA for online service providers.

Swiss law generally treats online contracts similarly to offline contracts, emphasising consent, transparency, and contractual obligations, without introducing separate legal regimes for digital commerce. Switzerland follows a "technology-neutral" approach.

### 1.2.2 Key Obligations for Online Contracting

**Key Obligations for Businesses Contracting Online in Switzerland**

Under Swiss law, businesses engaging in online contracts must comply with obligations primarily derived from the CO, the FADP, the FAUC and sectoral rules. Key obligations include the following.

- Contract formation and clarity – offers, acceptance and terms must be clear and unambiguous (CO, Articles 1–10, and specifically 7). Businesses must ensure users understand the terms before concluding contracts.
- Electronic signatures – where legally required, qualified electronic signatures (as opposed to other non-qualified electronic signatures like Docusign) can replace handwritten ones (ESigA, SR 943.03).
- Transparency and information duties – businesses must inform users about prices, contractual terms as well as data processing practices (CO, Articles 8 and 9, and FADP, Article 19). Note that Switzerland does not provide for mandatory withdrawal rights of consumers (as, eg, provided for consumers in the EU).
- Data security obligation – adequate technical and organisational measures are required to safeguard personal data collected during transactions (FADP, Articles 7–10).
- Commercial practices under the UCA (Unfair Competition Act) – pursuant to the UCA, whoever offers goods, works or services online, must (i) provide clear and complete details of his/her identity and contact address, (ii) indicate the individual steps that lead to the contract being concluded, (iii) provide suitable means for correcting input errors before submitting the order, and (iv) provide immediate online confirmation of the customer's order. Furthermore, misleading advertising practices and

unfair/improper terms are generally prohibited under the UCA (see UCA, Articles 2 and 8).

#### 1.2.3 Formation of Contracts Online

In Switzerland, the conclusion of online contracts is generally governed under the CO. The law does not impose a general requirement for written form, meaning contracts can generally be concluded electronically (CO, Articles 1–10). Key points include the following.

- Electronic signatures – the ESigA states that qualified electronic signatures are equivalent to handwritten signatures, enabling legally binding contracts online where a signature is required by law. Simple or advanced electronic signatures may suffice depending on risk and contractual requirements, but do not provide the same degree of equivalence.
- Consent and offer/acceptance – any online contract conducted requires a clear offer and a clear acceptance (CO, Articles 3 and 7). Clickwrap or checkbox agreements are generally considered valid if the terms are presented clearly and acceptance can be evidenced with a clear affirmation.
- Information duties – businesses must provide essential contractual information, such as the price and performance terms, ensuring informed consent (CO, Articles 8–9; FADP Articles 13–15). Note that Switzerland does not provide for mandatory withdrawal rights of customers (as, eg, provided for consumers in the EU).

Swiss law emphasises flexibility and functional equivalence with offline contracts, differing from EU directives mainly by allowing a broader use of electronic forms with less prescriptive procedural requirements.

## 2. Software Licensing and "As a Service" Provision

### 2.1 "On Premise" Licence Models Rather Than SaaS Solutions

Despite the growth of cloud-based SaaS solutions, many organisations continue to use on-premise licence models due to several key factors.

- Compliance and supervisory authorities – customers with sensitive or regulated data (eg, in finance, healthcare or government) prefer local control to ensure compliance with supervisory authorities and/or to guarantee a higher degree of data control to their customers (as a selling argument). While the Swiss FADP generally permits outsourcing of data abroad, if certain conditions are met, the aforementioned reasons can still make companies prioritise on-premise solutions.
- Technical control and customisation – on-premise deployments allow deeper customisation, integration with legacy IT-systems, and control over update schedules.
- Commercial cost predictability – some organisations favour one-time licence fees over recurring SaaS subscriptions, particularly for long-term usage.
- Performance and reliability – critical systems with high availability requirements may benefit from local infrastructure, avoiding dependence on internet connectivity or third-party cloud providers.
- Legal and regulatory compliance – certain Swiss regulations may require data to remain within national borders, making on-premise solutions preferable. For instance, FINMA (the Swiss Financial Market Supervisory Authority) expressly requires data of financial institutions to remain stored/accessible on Swiss soil.

### 2.2 Suspension Rights

In Switzerland, software suppliers commonly include suspension clauses in licence or service agreements (in particular in cloud-based SaaS solution-agreements). Key triggers include the following.

- Non-payment – failure to pay licence fees, subscription charges, or other contractual payments is the most common suspension trigger.
- Breach of contract – violations of licence terms, such as unauthorised use, exceeding user limits or violation of usage restrictions, can sometimes trigger suspension.
- Security or compliance risks – suppliers may suspend access if the licensee's system poses security threats (eg, malware risks) or obviously fails to comply with data protection obligations.

- Regulatory or legal obligations – compliance with court orders, law enforcement requests or regulatory requirements may sometimes justify temporary suspension.

Suspension rights are usually defined in the relevant contract, but default law provisions of the CO would also provide for such rights in certain instances. Suspension rights should be proportionate and notified to the customer. They often include curing periods to mitigate the disputes.

### 2.3 Audit Rights

#### Customer Audit Rights

Customers often request audit rights to ensure compliance with licence terms, service levels, and data protection obligations. Common requests include verification that the supplier is not overcharging and that usage matches the agreed licence scope, Service Level Agreement (SLA) adherence and that the supplier's technical and organisational measures comply with the FADP.

#### Supplier Audit Rights

Suppliers seek audit rights primarily to ensure proper use of software or services by the customer. Common triggers include licence compliance (verifying that the customer is not exceeding user numbers or copying software beyond the agreed scope), security and infrastructure or other contractual obligations.

In Switzerland, audit rights are typically contractually negotiated, should be proportionate, limited in frequency, and conducted with notice to avoid disputes. In a regulatory context, audits by supervisory authorities may sometimes be imposed by mandatory law especially in the case of specific events. Furthermore, in the course of a dispute (pending or pre-litigative measures), an audit could also be ordered and enforced by a judge.

### 2.4 Escrow Provisions

In Switzerland, software escrow arrangements are increasingly included in contracts, particularly for critical business applications, SaaS, or on-premise enterprise systems. An escrow agent ensures that the customer can access the source code or essential components, if the supplier fails to maintain, support, or continue operations, mitigating business continuity and dependency risks. Escrow provisions are contractually agreed, not expressly mandated by Swiss law. Commonly stated trigger events include supplier insolvency, breach of support obligations, or prolonged unavailability of updates. Contracts usually specify which source code, documentation, and materials are deposited, and under what conditions the customer can access them. Independent third-party escrow agents with technical knowledge are often used to safeguard the materials and to ensure enforceability.

While not legally required, escrow is considered best practice for high-value or mission-critical software or when the licensor is in a financially unstable position.

### 2.5 Commitments Regarding Ongoing Availability of Saas Solutions

In Swiss cloud-based SaaS (Software as a Service) contracts, providers typically give service availability commitments to ensure reliability and continuity. These are generally expressed as SLAs and may include uptime guarantees (commonly 99–99.9%, excluding scheduled maintenance), maintenance and downtime notification, incident response and resolution mechanisms, data backup and recovery and remedies for non-compliance (eg, service credits or partial fee reductions).

Swiss law does not impose specific availability standards; rather, a general standard of diligence and care (Article 398, CO). However, contractually agreed SLAs become a contractually binding framework within the contract. SLA terms are negotiated based on criticality of the service and customer risk tolerance.

## 3. Artificial Intelligence

### 3.1 AI Legislation and Regulation

#### 3.1.1 General Legislative Regime for AI

Switzerland does not yet have a specific, comprehensive AI law. The use and development of AI are primarily governed by existing sectoral legislation.

- Data protection – the FADP applies to personal data processed by AI systems.

- Civil liability – the CO and CC govern liability for damages caused by AI.
- Sectoral regulations – AI in healthcare, finance or transport may be subject to sector-specific regulatory frameworks.

The Swiss Federal Council published a strategy paper on AI (2020) promoting innovation while emphasising ethics, transparency, and human oversight, but legally binding AI-specific obligations are still limited. In March 2025, the Swiss Federal Council joined and ratified the Council of Europe's AI Framework Convention, and committed to adapt standards of this convention into Swiss law accordingly over time. While this ratification has not yet taken effect, it will primarily apply to state actors at the federal level and would only in exceptional cases have a horizontal effect on private parties (eg, where fundamental rights are at stake and must be reflected in contracts with governmental bodies).

#### 3.1.2 AI-Related Lower-Level Regulation

While Switzerland has no general AI law, sector-specific regulations can impose requirements on AI use.

- Healthcare – AI in medical devices is regulated, eg, under the Medical Devices Ordinance (MedDO, SR 812.213) and Swissmedic guidelines, requiring safety, performance and risk management.
- Finance – financial institutions using AI must comply with various FINMA regulations on risk management, transparency and model validation.
- Transport and safety-critical systems – AI in autonomous vehicles or aviation is subject to Federal Roads Office (FEDRO) and Swiss Civil Aviation Authority (FOCA) standards.
- Data protection and ethics – all sectors must comply with the FADP and should adhere to ethical principles for fairness, transparency and accountability, as recommended by the Federal Council's AI strategy.

#### 3.1.3 AI-Related Self-Regulation

Many Swiss companies self-regulate AI development and use due to the absence of comprehensive AI-specific legislation. Self-regulation typically involves internal policies and guidelines, ethical AI principles, risk management frameworks, and human oversight mechanisms, data governance (FADP), standards and best practices, adoption of international standards (eg, ISO/IEC 42001 on AI management) and sectoral guidelines, and internal audit to review algorithmic performance, bias and security.

### 3.2 Contractual Requirements With Respect to AI

#### 3.2.1 Key Requirements Sought by Customers

When contracting AI solutions, Swiss customers typically seek assurances covering risk, performance and compliance. They mostly focus on transparency and explainability, compliance with data protection, performance and accuracy, liability and indemnifications for errors, harm, or regulatory breaches caused by AI outputs, audit and monitoring rights, and ethical and regulatory compliance. Contracts often combine technical, legal and ethical safeguards to manage the inherent risks of AI solutions.

#### 3.2.2 AI-Related Liabilities in Contracts

In Switzerland, AI liability is primarily addressed contractually, since no AI-specific law exists. Key approaches include the following.

- Allocation of responsibility – contracts specify whether the supplier or customer bears risk for errors, biased outputs, or harm caused by AI.
- Warranties and performance guarantees – suppliers often warrant compliance with contractual specifications, accuracy thresholds, and regulatory obligations.
- Indemnification clauses – suppliers may agree to indemnify customers for damages, regulatory fines or third-party claims resulting from AI misuse or failures.
- Limitations of liability – parties often cap financial exposure, exclude indirect damages, and define triggers for liability.
- Audit and monitoring rights – customer oversight provisions mitigate risk and support liability enforcement.

### 3.3 Key Concerns of Providers

Providers of AI solutions in Switzerland face several legal, operational and reputational concerns.

- Liability risk – exposure to claims for errors, biased outputs, or regulatory violations.
- Data compliance – ensuring adherence to the FADP, particularly when processing personal or sensitive data.
- Intellectual property – protecting proprietary algorithms and balancing customer audit rights with confidentiality.
- Regulatory uncertainty – navigating sectoral rules (finance, healthcare and transport) and the absence of a unified AI law.
- Ethical and reputational risk – managing bias, transparency and fairness to maintain trust.
- Contractual obligations – meeting performance, uptime, and explainability commitments while limiting exposure through liability caps and warranties.

## 4. IT Services

### 4.1 Overlay of Requirements

Under Swiss law, there is no codified "IT services act". The provision of IT services is subject to a combination of general civil, commercial, IP and data protection laws.

The CO governs contractual relationships, including service agreements, outsourcing, SaaS, software development and maintenance contracts. Depending on the contractual structure, default law provisions of the CO relating to mandates, work contracts or mixed contracts may apply.

In addition, providers must comply with the FADP, where personal data is processed, including obligations relating to transparency, data security and processor arrangements. Sector-specific regulation may also apply on top. However, it is pertinent to mention that such regulation is mostly addressed to the customers of providers, which then try to shift/mirror these obligations in their contracts with the provider.

Intellectual property laws govern ownership and licensing of providers' software and deliverables.

Swiss unfair competition, export control and cybersecurity-related rules may further apply depending on the nature of the services provided.

### 4.2 Liability Clauses

A typical Swiss IT services liability clause addresses scope of liability, exclusions, limitations and allocation of risk between the parties. It usually includes liability for direct damages caused by breach of contract, gross negligence or wilful misconduct, while excluding liability for indirect or consequential damages such as loss of profit, loss of data, business interruption or reputational harm.

Liability is commonly capped, often by reference to fees paid under the agreement during a defined period (eg, 12 months). Under Swiss law, liability for unlawful intent (wilful misconduct) and gross negligence cannot be excluded in advance (Article 100, CO). Contracts regularly carve out certain damages from liability limitations (eg, for breach of confidentiality or data protection).

### 4.3 Warranties

Under Swiss law, IT services agreements typically include warranties relating to specific functionalities, ownership of intellectual property rights and non-infringement of third-party intellectual property rights, compliance and legal rights. Warranties are considered strict liability commitments irrespective of each party's fault.

Performance standards (eg, services to be provided with due care and professional diligence, in accordance with industry standards or service levels) are typically not addressed within a warranty section as they relate mainly to the quality of performance, which is considered part of the diligence and care of a service provider. Under Swiss statutory default law provisions of the mandate agreement (Article 398 et seq, CO), the duty of diligence and care is considered an inherent and mandatory duty of a service provider. It is not subject to a warranty. Nonetheless – especially under Anglo-American-negotiated contracts – parties do sometimes agree to represent and warrant performance standards. In this case, they mutually agree to uplift the performance level to a strict liability level (as a warranty).

From a data protection perspective, warranties commonly include compliance with the FADP and imple-

mentation of appropriate technical and organisational security measures.

Limitations and counter-exclusions to warranties are also common in practice (eg, conditions under which software must be used, and failure leads to forfeiting of warranties).

### 4.4 Agile Methodology

Agile contracting structures are common in Switzerland, especially for software development, SaaS implementation and digital transformation projects. Swiss law provides broad contractual freedom, allowing parties to structure projects using agile methodologies such as Scrum or Kanban. In practice, agile contracts are typically based on framework agreements combined with sprint-based statements of work (usually within a jointly used computer program, not on written paper), iterative deliverables and flexible change management procedures. Compared to traditional waterfall models, agile contracts focus more on governance, collaboration, prioritisation and acceptance processes rather than fixed specifications in advance.

Under Swiss law, the legal qualification depends on the substance of the arrangement. Depending on the degree of deliverable commitment, agile IT contracts may qualify as service contracts (little deliverable commitment), work contracts (clear deliverable commitment) or mixed contracts under the Swiss Code of Obligations. Careful drafting is important. In practice, too open agile contracts (with hardly any tangible specifications in advance) bear high potential for later disputes.

### 4.5 Payment Models

In Switzerland, IT services agreements commonly use a variety of payment models depending on the nature and complexity of the services. Typical structures include fixed-price models for clearly defined projects or milestone-based deliverables, and time-and-materials models where scope and requirements may evolve during the project.

## 5. Telecommunications and Networks

### 5.1 Telecoms Laws and Regulations

The key Swiss telecommunications law is the TCA supported by implementing ordinances and overseen by the Federal Office of Communications (OFCOM). It regulates market access, interconnection, spectrum use, and basic service obligations. Competition law under the Cartel Act also plays a major role, particularly regarding non-discriminatory access to infrastructure and prevention of abuse of dominance. Consumer protection rules require transparency in pricing and contract terms. The FADP is also highly relevant due to extensive personal data processing by telecom providers. Additional obligations may include lawful interception, emergency services access and roaming rules.

### 5.2 Telecoms Regulatory Bodies

The main telecom regulator in Switzerland is OFCOM, responsible for implementing the Federal Telecommunications Act, managing spectrum, numbering and supervising telecom operators.

The Federal Communications Commission ("ComCom") is an independent authority handling key decisions such as frequency allocation and infrastructure access disputes.

The Competition Commission ("COMCO") enforces competition law in the telecom sector, while the FDPIC oversees compliance with data protection rules under the FADP.

### 5.3 Telecoms-Related Regulated Activities

In Switzerland, regulated telecom activities include the provision of public telecommunications services (eg, fixed and mobile voice, and internet access), operation of telecommunications networks, use of radio frequencies, and assignment of numbering resources. Infrastructure-based services and certain wholesale/interconnection activities may also be subject to regulatory oversight under the TCA.

Generally, Switzerland follows a liberalised regime: no general telecom operating licence is required to provide most public telecom services. However, pro-

viders must register with OFCOM and comply with applicable regulatory obligations.

Licences or concessions are required for the use of scarce resources, such as radio spectrum (eg, mobile network frequencies), all of which are allocated by the Federal Communications Commission. Numbering resources are assigned by OFCOM. Additional authorisations or sector-specific approvals may apply for specialised services or infrastructure depending on technical and public-interest considerations.

### 5.4 Interconnection and Roaming Rules

In Switzerland, interconnection is regulated under the TCA and requires providers with significant market power to grant non-discriminatory, transparent and cost-oriented access to their networks. Interconnection agreements are generally negotiated commercially, but OFCOM and the ComCom can intervene in disputes and impose conditions if necessary to ensure fair competition and interoperability.

### 5.5 Consumer Protection Rules

Swiss telecom consumer protection is mainly based on the TCA, the UCA and general contract law principles under the CO. Providers must ensure transparent pricing, clear contract terms, and adequate pre-contractual information, including minimum contract duration, termination conditions, and any automatic renewal mechanisms. Contracts must be fair and not misleading. Unfair standard terms may be challenged under Swiss contract law and the UCA. Providers must also allow number portability and ensure service continuity rules are respected.

## 6. Intellectual Property Considerations

### 6.1 Background and Foreground IP

Under Swiss IT contracts, parties typically distinguish between “background IP” (pre-existing intellectual property) and “foreground IP” (newly created deliverables) through explicit contractual definitions. Background IP is usually defined as any IP owned or controlled by a party prior to the agreement or developed independently of it, and it generally remains with the originating party. Foreground IP is defined as IP created specifically in the course of performing the contract. In work-type contracts, clients often seek assignment of foreground IP upon creation or acceptance, while in service or SaaS models, IT-providers often retain ownership and grant usage rights only instead.

### 6.2 Types of IP

In Swiss IT and commercial contracts, the key IP rights typically addressed are copyrights, as it is central to software, source code, databases and software documentations under the Swiss Copyright Act (CopA, SR 231.2). Closely linked are licensing rights, which define how software and digital content may be used, modified and distributed. Patents are also relevant, for technical inventions, algorithms with technical effect or hardware-integrated software solutions. Trade secrets and know-how are also highly important in practice and often protected through confidentiality clauses rather than formal registration, especially for, eg, business processes. Trade marks are relevant where branding of IT-services or software products are involved. In some cases, design rights may be relevant for user interfaces or product aesthetics.

### 6.3 Use of Generic Know-How

Under Swiss IT contracts, ongoing use of generic or residual know-how is typically addressed through a “retained know-how” clause. Providers usually retain the right to use general skills, ideas, techniques and experience acquired during performance of the contract, provided this does not disclose the client’s confidential information or specific deliverables. Swiss law generally allows this distinction, as know-how is not a formally registered IP right but is protected mainly through contract and trade secret law.

### 6.4 Patent Claims

In Switzerland, patent filing activity has remained broadly stable over time, with a gradual long-term increase. Switzerland is a high-innovation jurisdiction, particularly in pharmaceuticals, medical technology, precision engineering and ICT-related fields. Patent protection remains an important tool in these sectors. In the IT and software space, however, patent claims remain comparatively limited, as pure software as such is not patentable unless it has a technical effect. Overall, patent activity is stable, with strong

sector-specific concentration rather than broad-based growth or decline.

### 6.5 IP and AI/Computer-Created Works

Under Swiss law, AI or computer-generated works are not explicitly regulated by a dedicated provision. Protection under the CopA requires a human intellectual creation with an individual character. Works generated autonomously by AI without sufficient human creative input in the prompts are generally considered not protected by copyright. Purely machine-generated outputs therefore typically fall into the public domain from a copyright perspective.

For other IP rights, such as patents or trade secrets, AI-assisted inventions may be protectable if they meet the relevant statutory criteria, but the inventor must be a human. In current practice, protection of such works is often achieved through contractual arrangements and trade secret protection rather than relying on copyright for AI-generated content.

## 7. Data Protection Considerations

### 7.1 Relevant Laws and Regulations for Data Protection

The main Swiss data protection law is the revised FADP complemented by the Federal Data Protection Ordinance (FDPO, SR 235.11). It sets core principles for lawful, proportionate and secure processing of personal data, supervised by the FDPIC.

Cybersecurity and information security obligations are mainly indirect, ie, arising from the FADP's security requirements and sector-specific rules (eg, telecoms, finance and critical infrastructure). The new Swiss Federal Information Security Act (FISA) applies to federal authorities and critical infrastructures.

Additional protections are found in the SCC, which sanctions unlawful access to data and cybercrime, and guidance from the National Cyber Security Centre (NCSC).

### 7.2 Data Transfer Restrictions

Under the FADP, transfers of personal data to third countries are restricted if the destination does not ensure an adequate level of data protection. The Swiss Federal Counsel maintains a list of adequate jurisdictions to which transfers are generally permitted.

If no adequacy decision exists, transfers can still be legitimised through safeguards such as data transfer agreements under the EU-standard contractual clauses (SCCs) (as has been also approved by the FDPIC with a Swiss finish), binding corporate rules (for intra-group transfers), or other contractual or organisational measures ensuring equivalent protection. In specific cases, explicit consent, necessity for contract performance, legal claims, or overriding public interest may serve as a justification for transfers in countries with no adequacy decision.

### 7.3 Information Security and Cybersecurity Standards

Swiss law does not impose mandatory use of specific security standards such as ISO 27001, NIS2, or CSA CCM. Instead, the FADP stipulates that controllers and processors must implement "appropriate technical and organisational measures" to ensure data security, based on a risk-oriented and state-of-the-art approach. ISO 27001 is widely used in practice as evidence of compliance, but it is not legally required.

Sector-specific rules may impose stricter obligations, particularly in banking, telecoms, healthcare, or critical infrastructure, where regulators may expect alignment with recognised standards. NIS2 does not apply in Switzerland directly, though Swiss companies operating in the EU may need to comply extraterritorially. The newly enacted Swiss FISA operates as the equivalent of NIS2 in the EU. It stipulates data security requirements for federal governmental entities and critical infrastructures.

Overall, Switzerland follows a principles-based approach: security measures must be appropriate to the risk, but organisations have flexibility in choosing the applicable framework to demonstrate compliance.

### 7.4 Information Notification Requirements

Under the FADP, security incidents involving personal data must be notified if they are likely to result in a high risk to individuals' rights or privacy.

- This covers personal data breaches such as unauthorised access, loss or disclosure of personal data.
- Notifications must be made to the FDPIC; sector regulators may also need to be informed in regulated industries (eg, FINMA must be notified of cyberbreaches occurring in regulated financial institutions).
- Notification must be made without undue delay; no fixed deadline is specified, but "as soon as possible" usually implies as soon as tangible and reliable forensic analysis is at hand. In Swiss practice, notification periods between five and ten working days can be seen, depending on the severity of the case.

Contractually, notification duties are often performed by the supplier (processor), but legal responsibility generally remains with the customer (controller).

## 7.5 Supply Chain Requirements

### 7.5.1 Risk Assessments and Due Diligence on Suppliers and Extended Supply Chains

There is no general Swiss statutory obligation requiring formal supplier or extended supply chain risk assessments across all sectors. However, under the FADP, controllers and processors must implement appropriate technical and organisational measures, which in practice requires risk-based due diligence when engaging IT suppliers and sub-processors. Overall, while not expressly mandated in detail, supplier due diligence is effectively required as part of compliance with Swiss data protection and sectoral risk governance standards.

### 7.5.2 Data Protection or Information/Cybersecurity Terms in Supply Agreements

Under Swiss law, there is a mandatory requirement to include data protection terms when a supplier processes personal data on behalf of a customer and sub-processors are also involved. Under the FADP, the relationship must then be governed in a data processing agreement (DPA) or equivalent contractual provisions. Such terms should usually regulate:

- subject matter, duration, nature and purpose of processing;
- types of personal data and categories of data subjects;
- obligations and rights of the controller;
- processor obligations to process data only on documented instructions;
- confidentiality;
- technical and organisational security measures;
- use of sub-processors; and
- assistance with data subject rights and breach notifications.

There is no general statutory requirement to include cybersecurity clauses beyond this, but the FADP requires "appropriate security measures" for any type of hired data processing with the help of processors, so it is typically implemented contractually. Sector-specific rules (eg, finance, telecoms and critical infrastructure) may impose further security and outsourcing provisions.

### 7.5.3 The Application of Laws Relevant to Supply Chains

Under the FADP, the customer (data controller) carries primary responsibility for ensuring lawful processing, including selecting suitable processors and ensuring appropriate contractual safeguards. However, the supplier (data processor) is also subject to statutory and contractual obligations, such as processing data only on instructions, ensuring confidentiality, implementing adequate security measures, and co-operating with the controller.

In addition, sector-specific regulations (eg, financial services, telecoms and critical infrastructure) may impose direct outsourcing, risk management, and security obligations on both parties.

# 8. Legislative and Regulatory Adaptation and Advancement

## 8.1 AI-Related Legal Adaptation

Switzerland is not expected to adopt a standalone AI law comparable to the EU AI Act. Instead, regulation will likely evolve in a sectoral and principles-based way, building on existing frameworks such as data protection, product safety, liability, and contract law. The Federal Council has indicated a preference for a

light-touch approach focused on innovation, with targeted rules for high-risk uses of AI. Alignment with EU developments is likely to remain important for cross-border compatibility.

### 8.2 Standards in Contract Drafting

Swiss IT contract standards have become more detailed and compliance-driven in recent years, mainly due to the FADP and increased cloud and outsourcing use. Key developments include more granular data processing agreements, clearer allocation of roles, stronger security and breach notification clauses, and broader audit and subcontractor controls.

### 8.3 Hyperscalers

Hyperscalers such as Microsoft, AWS and Google have made IT contracting in Switzerland more standardised and less individually negotiable. Customised requirements are mostly met with so-called "standard amendments", of which many exist, and hyperscalers tend to employ for similar scenarios encountered with many other customers. Overall, their influence has reduced contractual flexibility, but depending on the bargaining power/leverage of the respective customer. On the customer side, this has increased reliance on governance, compliance, and multi-cloud procurement strategies.

### 8.4 IP Evolution

Traditional IP concepts in Switzerland remain fit for purpose, but they are challenged by new technologies such as AI and data-driven services. For instance, machine-assisted inventions or data assets missing human authorship or inventorship create items not fitting into the existing IP-categories and may lack protection. While overall the author believes copyright, patent, and trade secret regimes still continue to provide a solid basis, contractual arrangements and trade secret protection will become more important to supplement the existing statutory IP rights.

## 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 Luke.Wilson@Chambers.com