COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Switzerland

TMT

Contributor

TIMES Attorneys

Martina Arioli

Partner | arioli@timesattorneys.ch

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Switzerland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

SWITZERLAND
TMT

1. What is the regulatory regime for technology?

There is no specific regulatory regime in Switzerland that governs technology, per se. Moreover, there are various statutory and regulatory frameworks pertaining to particular sectors or types of services such as telecoms or financial services that do contain requirements that have an impact on technology services. However, the Swiss legislator takes a technology-neutral approach.

2. Are communications networks or services regulated?

The main law governing the transmission of information by means of telecommunications techniques is the Telecommunications Act (TCA). The TCA and the Ordinances based upon the TCA have recently undergone revision, entering into force on 1 January 2021.

The aim of the TCA is to ensure that a range of cost-effective, high-quality, and nationally and internationally competitive telecommunications services is available to private individuals and the business community. The TCA shall, in particular: a) ensure that a reliable universal service is provided at affordable prices for the entire population in all parts of the country; b) ensure that telecommunications traffic is free from interference and respects personal and intellectual property rights; c) allow effective competition in the provision of telecommunications services; and d) protect users of telecommunications services from unfair mass advertising and from abuse associated with value-added services.

On the basis of the TCA, several Ordinances have been enacted and revised: the Ordinance on Telecommunications Services; the Ordinance on Telecommunications Installations; the Ordinance on the Addressing Resources of Telecommunications Services with modernized standards relating to short numbers; the Ordinance on Frequency Management and Radio Licenses, completely revised with technical adjustments; the Ordinance on Electromagnetic Compatibility; and the Ordinance on Fees in the Telecommunications Sector.

Further, the Federal Act on Surveillance of Post and Telecommunications and the respective Ordinance apply to communications services.

3. If so, what activities are covered and what licences or authorisations are required?

Due to the latest comprehensive revision of the TCA, the frequency spectrum may be used freely within, of course, the limits of the applicable regulations. Accordingly, there is no notification or authorization requirement for telecommunication service providers. However, addressing resources, and radio frequencies require a registration, and the use of mobile radio frequencies for the provision of telecommunication services and the provision of universal services still do require a license. Further, the revised TCA provides for a legal basis for frequency sharing and trading.

4. Is there any specific regulator for the provisions of communications-related services?

The Federal Communications Commission (ComCom), an independent commission with decision-making powers, is in charge of the regulation of the telecommunications market, of awarding the universal service licence, as well as radio communication licences for the use of the frequency spectrum, of determining access conditions and prices when telecommunications service providers cannot reach agreement, of the approval of the national numbering plans, and of the regulation of the methods of application of number portability and carrier selection.

The Federal Office of Communications (OFCOM) is formally part of the Federal Department of the Environment, Transport, Energy and Communications, and acts as the supervisory authority in the

communications sector. It is responsible for tasks relating to regulation and is the national authority in the areas of telecommunications, broadcasting and post, ensuring, in particular, the quality of the universal service and the public service.

5. Are they independent of the government control?

The above regulatory bodies are independent of government control. Decisions of the ComCom can be appealed to the Federal Administrative Tribunal based on, inter alia, the violation of federal law including the exceeding or abuse of discretionary powers, and the incorrect or incomplete determination of the legally relevant facts of the case.

Decisions of the Administrative Tribunal can be further appealed to the Federal Supreme Court based on, inter alia, the violation of federal law and the manifestly incorrect determination of the legally relevant facts of the case. Decisions of the Federal Administrative Tribunal regarding licences granted by means of public tender proceedings, and disputes regarding access to facilities and services of providers with a dominant position, cannot be deferred to the Federal Supreme Court.

6. Are platform providers (social media, content sharing, information search engines) regulated?

No, not specifically. In particular the recent revision of the TCA does not contain any provisions that regulate platform providers, however, the Federal Council did identify the need for clarification. EU regulations do not apply in Switzerland.

7. If so, does the reach of the regulator extend outside your jurisdiction?

N/A.

8. Does a telecoms operator need to be domiciled in the country?

No. The market for telecommunications services in Switzerland has been liberalized for more than 20 years. Foreign telecoms operators are free to enter the Swiss market. Moreover, the development towards an IP-based network offered by new and/or foreign telecoms operators fuels competition.

9. Are there any restrictions on foreign ownership of telecoms operators?

In general, there are no restrictions; however, in the absence of any international obligations to the contrary, the ComCom may prohibit undertakings incorporated under foreign law from providing telecommunications services in Switzerland, unless reciprocal rights are granted. This has not changed with the revision of the TCA.

10. Are there any regulations covering interconnection between operators?

The TCA requires providers with a dominant market position to provide access to other providers in a transparent and non-discriminatory manner, at cost-oriented prices. The same applies to universal services providers. Dominant telecoms operators must grant other telecoms operators access to their facilities and services in a transparent and non-discriminatory manner at cost-oriented prices as regards: 1) full unbundled access to the local loop using the full frequency spectrum of the twisted metallic pair; 2) the rebilling of fixed local loops; 3) interconnection; 4) leased lines; and 5) access to cable ducts, provided they have sufficient capacity. The TCA does not extend the unbundling of “the last mile” and remains limited to copper lines. Dominant telecommunication services providers must inform on their conditions and prices separately for each of their individual access services.

If the providers in question are unable to negotiate an amicable settlement with regard to access conditions within three months, the dispute may be brought before the ComCom, which decides based on a proposal made by the OFCOM.

11. If so are these different for operators with market power?

Cf. question 4.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

Basic telecommunication services must be available to the entire Swiss population in all regions. To ensure that these are affordable, reliable, and of good quality, the ComCom grants a licence for providing universal service within a tender process. Telecommunication services providers are essentially free to determine the general

terms and conditions applicable to consumers, in particular roaming charges, which are relatively high in Switzerland. Effective from July 2021, the Federal Council has included a number of new provisions in the OTS designed to increase price transparency and consumer choice in international roaming. Maximum charges apply only to certain telephony services provided by the universal services provider Swisscom, as well as value-added services. Further, telecommunication services providers must comply with the principle of secrecy of telecommunications as well as data retention obligations.

The core aims of the recent partial revision of the TCA include the strengthening of consumer protection, the protection of children and young people, the principle of network neutrality, the restricted access to the "last mile" for fibre optic connections as well as the promotion of competition. Further, the Federal Act on Unfair Competition has been revised in order to tighten the requirements for telephone marketing, and to introduce the possibility for the public prosecutor's office and courts to revoke or block domains and telephone numbers that have been used in violation of the Act on Unfair Competition or the Price Disclosure Ordinance.

Lastly, the Federal Price Supervisor monitors price developments and prevents or eliminates the abusive increase and retention of prices based upon the Federal Price Supervision Act, and the COMCO takes measures against unlawful restraints of competition where retail prices are affected, based upon the Cartel Act of the COMCO.

13. What legal protections are offered in relation to the creators of computer software?

Pursuant to the Federal Copyright Act, computer software is deemed a copyrighted work. Unless it is a computer-implemented invention that solves a technical problem, computer software cannot, as a rule, be patented. Computer software may also be protected as trade secret under the Federal Act Against Unfair Competition and under the Swiss Criminal Code. Design elements may be registered under the Federal Design Act.

14. Do you recognise specific intellectual property rights in respect of data/databases?

Even though there have been several attempts to do so, Switzerland has never implemented a database right similar to the one introduced by the Database Directive in 1996. Accordingly, there is no sui generis protection of databases in Switzerland. Swiss law only provides to database owners very limited protection under the Swiss Copyright Act and, also to a very limited extent, the Federal Act against Unfair Competition.

According to Swiss copyright law, databases only qualify for protection if they qualify as original databases. The requirement of originality demands that a database must constitute an intellectual creation by virtue of the selection or arrangement of its contents in order to enjoy copyright protection. As soon as a database serves its true purpose, i.e. is comprehensive, it fails to meet the criteria of originality. Consequently, the majority of the databases are not protected under copyright law even if substantial investments have been made to produce them.

15. What key protections exist for personal data?

Given that Switzerland is not a member of the EU nor the EEA, the General Data Protection Regulation (GDPR) does not apply in Switzerland. The revised Federal Act on Data Protection Act (FADP) will enter into force in September 2023, containing provisions similar to the GDPR pertaining to the principles of data processing and accountability, as well as the transfer of data to countries without an adequate level of data protection. The FADP aims to protect the privacy and the fundamental rights of persons when their data is processed by private persons or federal bodies. The FADP requires, amongst others, that personal data may only be processed lawfully, that its processing must be carried out in good faith and must be proportionate and that the purpose of its processing must be evident to the data subject.

In addition, industry sector-specific regulatory requirements governing data security and data protection matters may apply.

16. Are there restrictions on the transfer of personal data overseas?

Personal data can be transferred outside of Switzerland. If the country to which personal data shall be transferred does not provide for an adequate level of protection, the parties must either obtain the consent of each data subject individually or put measures in place to ensure that the data is adequately protected in the relevant jurisdiction, such as sufficient contractual guarantees, or binding corporate rules (BCR), provided the processing takes place within a legal entity or among legal entities

under common control and all involved parties are subject to the BCR.

The Schrems II decision by the European Court of Justice of July 2020 does not apply in Switzerland; however, it of course has a great impact on the validity of cross-border transfers based upon Standard Contractual Clauses (SCC) given that Switzerland follows the EU regime. For cases of cross-border outsourcing, the Federal Data Protection and Information Commissioner (FDPIC) has adopted the SCC issued by the EU Commission in June 2021. In order to cover Swiss law, the FDPIC stipulates some (minor) changes to be made to the SCC.

Under the revised FADP, the parties no longer need to notify the FDPIC if the cross-border transfer is based upon the SCC or BCR.

17. What is the maximum fine that can be applied for breach of data protection laws?

The maximum fine for breach of certain obligations under the revised FADP is CHF 250'000. This may seem less deterrent at first glance compared to the fines of up to EUR 20 million or up to four percent of the worldwide annual turnover according to the GDPR. However, the GDPR fines are directed against the respective company, whereas the fines under the revised FADP are directed against the responsible natural person acting intentionally – and may lead to an entry in their criminal record. This difference stems from the fact that in Switzerland – unlike in the EEA area – there is no actual procedural law for administrative sanctions of a penal nature. Noteworthy is also that not every violation of the FADP is criminally sanctioned but rather only specific ones such as the violation of the duty to inform and provide access, the obligation to cooperate with the supervisory authority FDPIC, the duty to inform about automated individual decisions, the failure to comply with an order of the FDPIC, violations of data security and export restrictions, as well as the inadequate appointment of the processor or the breach of professional secrecy.

18. What additional protections have been implemented, over and above the GDPR requirements?

The GDPR does not apply in Switzerland. The FADP does not go beyond the GDPR.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

To date, there are no statutory provisions that apply specifically to cloud-based services.

For financial services, the regulatory requirements of the FINMA Outsourcing Circular 2018/03 of the Swiss Financial Market Supervisory Authority FINMA for outsourcing by banks, securities dealers, insurance companies, Swiss branches of foreign banks, securities dealers and insurers that are subject to FINMA supervision applies mutatis mutandis. The Outsourcing Circular 2018/03 sets out provisions on the selection, instruction and control of suppliers, including a comprehensive audit right, as well as provisions to secure availability of data. It also prescribes the contents of the outsourcing agreements, i.e. in cloud services contracts.

Article 321 of the Swiss Criminal Code obliges certain professionals such as medical staff, attorneys, notaries, auditors, members of the clergy, and their aides to professional secrecy. Any disclosure of confidential information that has been confided to them in their professional capacity or which has come to their knowledge in the practice of their profession is deemed a violation of the criminally sanctioned professional secrecy. IT providers are typically deemed aides (auxiliaries) to the aforementioned professions. Accordingly, they are subject to the same secrecy obligations. It is thus advisable to explicitly emphasise this in a technology sourcing contract, including the procurement of cloud services. Further, the healthcare sector is subject to extended secrecy obligations that render additional safeguards in cloud contracts necessary.

For public procurement, the processes set out in federal and cantonal public procurement laws need to be complied with. Depending on the value of the project (threshold), a competitive tender process is mandatory: open procedure; selective procedure; or invitation procedure. A direct award is only permitted in exceptional circumstances. Public procurement law applies not only to governmental bodies but also to private companies in the context of the provision of public services. The public procurement laws recently have undergone a paradigm shift from favouring the most economic tender to the best tender in terms of quality.

The Federal Council has issued its cloud strategy in 2020 in its struggle to digitally transform public services.

20. Are there specific requirements for the validity of an electronic signature?

Electronic signatures are regulated by the Federal Electronic Signature Act. An electronic signature essentially confirms the identity of the person signing and the traceability of the signed information, i.e. the subject of the signature and whether the content has been changed since it was signed.

Four different forms of electronic signature are distinguished, each with different technical characteristics: The 'simple' electronic signature; the advanced electronic signature; the regulated electronic signature; and the qualified electronic signature. Under Swiss law, only the qualified electronic signature, which is provided with a qualified electronic time stamp, is equivalent to a handwritten signature in accordance with article 14 para. 2bis of the Swiss Code of Obligations. The qualified electronic signature must be issued by a recognized provider of certification services. The Swiss Accreditation Service accredits the recognition bodies, which in turn are responsible for recognizing providers of certification services. There are currently only four recognized providers of certification services in Switzerland: Swisscom (Schweiz) AG, QuoVadis Trustlink Schweiz AG, SwissSign AG and the Federal Office of Information Technology, Systems and Telecommunication (FOITT).

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

Article 333 of the Swiss Code of Obligations (CO) stipulates that if the employer assigns its business or a business unit to an acquirer, the employment relationship of any employee affected automatically transfers to the acquirer, unless the affected employee objects to such transfer. This also applies to mergers, splits or asset transfers in accordance with Article 27 of the Swiss Merger Act. The previous employer is obliged to inform or consult with the employees' representatives or, if there is no representation, with the employees themselves in good time before the transfer takes place (Article 333a CO). The employment agreements are automatically transferred to the acquirer on essentially all existing terms and conditions, including benefits granted under the employment agreement or based on a collective bargaining agreement, as well as accrued holiday entitlements. After the transfer, the acquirer can modify the employment terms. The former employer and the acquirer are jointly and severally liable for an employee's claims that (i) are due prior to the transfer, or (ii) will become due up to the date the employment relationship can effectively be terminated or until its actual termination based on the employee's objection to the transfer. If the outsourcing agreement entails the transfer of business offshore, the parties need to assess whether the employment contracts of the affected employees actually transfer by operation of law given that Article 333 CO only applies if the business concerned preserves its identity post-transfer.

Assets and third-party contracts do not automatically transfer. Accordingly, the outsourcing contracts needs to specify the transfer. Further, it is strongly recommended to register transfers of trademarks and patents in the respective registries administered by the Swiss Federal Institute of Intellectual Property as soon as possible.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

The general liability rules apply to the use of new technologies. Pursuant to Swiss liability law, only a natural or legal person can be held liable, and not a machine or robot. Liability for the operation of autonomous information technology systems must always be linked to the act or omission of a person capable of committing a tort, even if the machine acts without the direct supervision of the person. Moreover, from today's perspective, it is difficult to attribute to autonomous AI systems attributes that are prerequisites for assigning responsibility in legal transactions. Machines do not appear to be capable of acting intentionally (with knowledge and will), negligently (without considering the consequences of their action due to carelessness in breach of duty), or culpably (personally reproachable), nor of developing a capacity for judgment (subjective capacity for insight, capacity for forming a will, and capacity for implementing the same). However, it cannot be excluded that the Swiss legislator may, at a point in time, introduce a new special strict liability applicable to AI systems. This means that a damage caused by an AI system is attributed to a specific person, regardless of fault. It will typically be that the person who benefits the most from the AI system shall also assume the associated risks.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

(a) obligations as to the maintenance of cybersecurity; and

Switzerland does not have a specific comprehensive regulation on cybersecurity. Provisions of general statutes apply, such as the Swiss Criminal Code, the FADP, the TCA, etc.

Under the revised TCA, telecommunication services providers are obliged to combat unauthorized manipulation of telecommunications equipment, for instance by rerouting or preventing connections or by suppressing information. Cyber-attacks are exclusively defined as manipulations through telecommunications transmissions, such as the distribution of malicious software or the impairment of web services (so-called DDoS attacks). Physical access and backdoors in hardware and software are not covered.

The Swiss Financial Market Supervisory Authority (FINMA) has published a supervisory notice on the obligation for the banks, insurance companies and other institutions under its supervision to report cyber-attacks.

Under the revised FADP, data breaches must be reported to the FDPIC as soon as possible, however, only if there is a high risk of negative consequences for the data subjects concerned.

On 19 April 2018, the Federal Council adopted the "National Strategy for the Protection of Switzerland against Cyber-risks (NCS)" for the period 2018–2022. The strategy builds on the results of the previous NCS adopted earlier in 2012, and aims at further developing it. The objective is to minimise cyber-risks. The strategy encompasses new standardisation and regulations objectives, and lays the ground for discussions on minimal standards for cybersecurity and new notification duties for cyber-incidents.

(b) the criminality of hacking/DDOS attacks?

Hacking is criminally sanctioned by article 143bis and article 179novies of Swiss Criminal Code.

24. What technology development will create the most legal change in your jurisdiction?

Most likely artificial intelligence. Whilst the government deems the traditional liability regime sufficient to tackle the new challenges, the "human in the loop" question still needs to be addressed in more detail in order to allocate responsibilities adequately. Further, the need for regulation may arise in particular when AI applications affect fundamental and human rights, threaten market failure, or affect the realm of government action. In particular, Switzerland does not have strong anti-discrimination laws, and consumer protection remains a patchwork. Further, Switzerland will need to address how to implement the EU Artificial Intelligence Act, once enacted, into Swiss law in order to provide Swiss players with legal certainty.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

There is no specific legal provision that impedes economic development / commerce in Switzerland. However, Switzerland is not a member of the EU / EEA and, accordingly, EU regulations do not apply in Switzerland. Nevertheless, Switzerland closely monitors legislative and regulatory developments in the EU and typically follows suit, albeit with a considerable time lag due to the at times rather lengthy legislative process; the revision of the FDAP, which shall enter into force only on 1 September 2023, may serve as an example. On the one hand, the dual regimes may pose a challenge for players active in both the Swiss and the EEA market.

26. Do you believe your legal system specifically encourages or hinders digital services?

Switzerland maintains a rather pragmatic and liberal approach to regulation which may be deemed to have an encouraging effect on digital services. Further, the technology-neutral stance may be deemed to enhance legal certainty: the legal framework shall not be geared to individual technologies but should rather treat comparable activities and risks in the same way as a matter of principle, wherever possible and sensible. However, regulatory requirements in particular enacted by FINMA may be subject to change which may create legal uncertainty. For example, FINMA changed its view on how to treat crowdfunding over the course of the years and entertained at times rigid interpretations of general legal provisions pertaining to money laundering. On other issues, authorities have given helpful and timely guidance on how to interpret existing provisions in view of technological developments.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

Cf. question 1.

Contributors

Martina Arioli
Partner
arioli@timesattorneys.ch