The Legal 500
COUNTRY COMPARATIVE GUIDES 2020

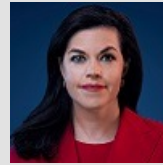# The Legal 500 Country Comparative Guides

Switzerland: TMT

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 here

Contributing Firm

NIEDERER KRAFT FREY   Niederer Kraft Frey AG

Authors

Clara-Ann Gordon
Partner
The Legal 500
Clara-ann.gordon@nkf.ch

1. **What is the regulatory regime for technology?**

   Switzerland pursues a bottom up strategy with regard to technology regulation. Technology can be developed without restrictions, as long as it adheres to the current law.

2. **Are communications networks or services regulated?**

   Under Swiss law the Telecommunications Act (TCA) regulates communications networks and services. The TCA sets forth the requirements of a telecommunication service provider, licence for the universal service, radio communication license, obligations of dominant providers, confidentiality and data protection obligations. A telecommunication provider is a person/company, who/which transmits information by means of electrical, magnetic or other electromagnetic signals information to a third party. Any person providing telecommunications services has to notify the Federal Office of Communications (OFCOM). Additionally, for the use of radio communication frequency spectrum a license is necessary.

   The Federal Act on Radio and Television (RTVA) regulates the broadcasting, processing, transmission and reception of programme services using telecommunication techniques. Programme services are defined as a continuously offered sequence of programmes for the public.

   The OFCOM regulates the price setting, obligations and duties arisen of the supply of telecommunications services as well as licences requirements in the Ordinance on Telecommunication Services (OTS) in detail.

   Communications networks in households, within a company, group or between public institutions are not inside the scope of the regulation.

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

   The TCA covers the offering and provision of telecommunication services. A licence is only required for the rendering of universal telecommunication services, the use of the radio frequency spectrum and provision of radio or television programmes services.

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

   The OFCOM administers the telecommunication services and enacts detailed regulations. The OFCOM has designated an independent arbitration board for civil law disputes between customers and their telecommunications providers. (Art. 42, 43 OTS).

5. **Are they independent of the government control?**

The OFCOM is not independent of the government control. However, the Independent Complaints' Authority for Radio and Television (ICA) rules on complaints against Swiss radio and television providers and violations of the RTVA and other applicable laws.

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

Platforms are not specifically regulated under Swiss law. However, the Federal Act on Data Protection (FADP), provisions regarding youth protection, unfair competition law and the TCA, if the social media platform is qualified as a telecommunication provider in the sense of the TCA, must be adhered to.

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

No.

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

The operator does not have to be domiciled in Switzerland. Foreign providers have to designate a correspondence address in Switzerland, to which notices and orders can be legally delivered. In the absence of international treaties, the OFCOM can prohibit a foreign operator from providing telecommunications services in Switzerland unless reciprocal rights are granted.

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

If a foreign operator supplies value-added services, the provider must operate the service from a headquarters or branch office in a state contracting to the Lugano Convention. Art. 37 OTS.

10. **Are there any regulations covering interconnection between operators?**

Interconnection between operators are subject to competition law. Interconnection may results in a position with market power. Providers with a licence for the universal supply are obliged to interconnection.

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

Operators with market power have to give access to their facilities and services to other operators at transparent and cost-oriented prices. Art. 11 TCA. This includes:

- fully unbundled access to the local loop;
- fast bit stream access for four years;
- rebilling for fixed network local loops;

- interconnection;
- leased lines;
- access to cable ducts, provided these have sufficient capacity.

A copy of the agreement needs to be filed with the OFCOM.

Services can be bundled, but must be offered separate as well, unless the sole offer of the service can only be supplied due to technical, economic, quality or safety reasons in a bundle. Art. 12 TCA.

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

For the universal supply, the Swiss Federal Council fixes a price ceiling. Art. 17 TCA.

The operator has to inform the customer free of charge, if a higher tariff rate is charged for a specific connection or call.

Mobile network providers have to inform their customers in writing about international roaming fees for calls to Switzerland, incoming calls, on-site calls, sending of SMS and data transmission.

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

The creators of computer software are legally protected under the Copyright Act (CopA). A computer programme is defined as a work in Art. 2 (3) CopA, if it fulfils the perquisite of an intellectual creation with individual character. Due to the doctrine individuality means that it is nearly impossible, that a third person will independently discover the same solution. Copyright protected is the concrete programme code, the sequences, structure, interface of the software, but not the basic idea or underlying procedures such as algorithms. The copyright protection expires 50 years after the death of the creator. Art. 29 (2)a CopA.

Software is patentable if it is new, inventive and technical. More precisely, it has to solve a specific technical task by technical means, for example the control of a technical procedure. The protection offered to software creators is similar to the protection granted in the EU.

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

Databases may be copyright protected, if the selection and arrangement of data/information collected is an intellectual creation of individual nature.[1] In the light of this, there are no specific intellectual property rights. Databases can be protected contractual between the parties pursuant to the Code of Obligation. Furthermore, Art. 162 of the Swiss Criminal Code (SCC) stipulates fines and imprisonment, if the accused business or factory secrets of

databases, that have been entrusted to him by law or contract.

[1] Rolf h. Weber. Datenbankrecht- Regelungsbedarf in der Schweiz ?. In Weber, Rolf H. Hilty, Reto M. (Hrsg.). Daten und Datenbanken, Rechtsfragen zu Schutz und Nutzung.Schulthess Polygraphischer Verlag Zürich,1999. S. 63

15. **What key protections exist for personal data?**

The FADP sets forth the definition of personal data, and the rights of data subjects.

Personal data is any data which allows to identify a specific person. Even if the person is only identifiable with the context of the information, the data is considered to be personal data.

Personal data can only be processed for the purpose indicated at the time of collection, which is evident from the circumstances or the purpose provided for by law. The collection and the purpose of processing must be evident to the data subject. Swiss Law defines "processing data" as any operation with personal data. This includes storing, use, revision, disclosure, archiving or destruction of data.

The processing has to be lawful, in good faith and proportionate. (Art. 4 FADP) Personal data has to be protected by technical and organisational measurements against unauthorized processing. (Art. 7 FADP) This may include access and processing documentation. The data subject has the right that incorrect data is corrected or destroyed. Art. 5 FADP. In addition, any person can request information from the controller of a data file, whether data concerning him is being processed.

A private data processor cannot process personal data against the explicit will of the data subject, unless there is a reason for justification. The processing is lawful without explicit consent of the data subject, if it is in connection with the performance of a contract, credit assessment, to get in touch with the data subject etc.

With regard to sensitive personal data and personality profiles, the controller of the data must inform the data subject about the content of the data file, purpose of processing, and disclose data transfers. Sensitive data contains information about religious, ideological, political, trade union-related views or activities, health, intimate sphere or racial origin, social security measures, administrative or criminal proceedings and sanctions.

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

If the personal rights of the data subject are infringed or at risk, especially through lack of equivalent legal protection, the transfer of personal data abroad is prohibited (Art. 6 FADP). Basically, the foreign jurisdiction has to grant at least the same level of protection as Switzerland or the protection is guaranteed through the receiver.

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

    The data protection law does not set forth a maximum fine. However the maximum fine as set out in Art. 106 SCC 10'000 CHF applies.

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

    As Switzerland is not a member state of the EU, it is not obliged to implement the GDPR. However, even after the GDPR coming into force, Switzerland continued to be considered as a country with a data protection law level equivalent to the one in the EU. Moreover, currently the FADP is being revised and aligned with the provisions of the GDPR.

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

    There are no laws or provisions relating specifically to cloud-based services. Cloud-based services are subject to the FADP. Cloud user have to ensure that the cloud provider as a third person processing data guarantees data security as set out in the FADP. The cloud user has to ensure that the cloud provider has technical and organisational measurements to protect personal data from unauthorized processing and that the data subject can exercise his right to information according to Art. 8 FADP and the right of deletion and correction to Art.5 FADP. Moreover, there are some industry-specific guidelines.

    It is imperative to keep in mind, that storing data in the cloud may be qualified as a transfer of data abroad, because the server of the cloud or suboperators is abroad. In this event Art. 6 FADP applies, which means that the cloud user has to ensure adequate protection in order to prevent serious risk to the data subject's personality.

    [2]
    https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html

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

    In Switzerland a qualified electronic signatures with a qualified time stamp is recognised as being equivalent to a handwritten signature. The Swiss Electronic Signature Act (ZertES; SR 943.03) defines a qualified electronic signature. Only natural persons are eligible to use the qualified electronic signature as an equivalent to the handwritten signature. Only a certification authority can generate an electronic valid signature. As regards the process: the person, who would like to register his signature, has to prove his identity with official documents at the certification office. Due to Covid-19 an electronic signature can be registered through real time audio-visual identity verification. Authorized certification offices can be found on the government's website[3].

[3] https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html

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

    The outsourcing of IT-services does not automatically by law transfer any employee, asset or third party contracts to the outsourcing supplier. However, the parties may agree in the outsourcing contract to transfer assets, take over employees and third party contracts. Under the specific circumstances, the consent of the affected employees or third party may be necessary.

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

    Swiss law has no specific liability scheme for damages caused by A.I. To determine the liable person, the cause of the malfunction has to be identified. If the malfunction results from the structure of the A.I., inadequate training or training data the producer is liable. However, if the damage arises from an operating error, e.g. entering unsuitable data, or if the A.I. software was used for another purpose than the one for which it was originally designed, the company using it, is liable for damages.

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

    There is no law governing cybersecurity in the private sector. 2018 the Swiss Federal Council established a national centre for cybersecurity, which is the first point of contact for the public, industry and public authorities on cyber security related issues.

    The Swiss Criminal Code punishes the unauthorised disclosure of/access to data with imprisonment of up to 5 years or a fine. Art. 143[bis] SCC criminalises unauthorised intrusion into data systems. This crime is only sanctioned by request with a fine or imprisonment.

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

    Self-driving cars, A.I. selections systems and personal identification/tracing application will not only change our daily life, but also the legal system. Especially the debate about liability of A.I. tools will force to develop a new liability scheme to ensure legal certainty and clear guidelines in future. Currently errors can still be traced, but in the future, this may not be possible anymore. Without the ability to define the cause of the damage, the present tort low will lose its relevance/applicability. A federal project group recently denied revising the Swiss liability law with regard to A.I..

The increasing collection of data by companies and the public administration, and the creation of profiles based on this data without the knowledge of the concerned person, demands for a restrictive data protection regime. Although many people are not aware what impact and power the collected data has in our daily life, it is imperative that private life's are protected more effectively by law. For instance data collections by virtue of smart household appliances, which exchange with each other sensitive data about the data subject's lifestyle, health condition and activities is stored. In fact, the enormous collection of data is an invisible invasion into privacy.

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

   According to the World Bank's Economic Profile Switzerland the requirements and time to found a company, obtaining a building permission and investor protection complicate economic development and commerce in comparison to other countries. Admission restrictions are mostly found in the medical and food sector. Since Switzerland is a rather small country, the market is not so large. Therefore, export of products is a common way to do business. This means that EU directives may also be important and apply indirectly to Swiss companies.

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

   The Swiss legal system and the government do not prevent inventive activities. Research and developers have a wide leeway to establish new technology forms and digital services. The aim is to asses, whether there are any black holes or risk for fundamental rights, rather than to hinder technological development. The current legal system is principal based and pursues a technological and competitive neutral approach. However, in our view there could be more governmental (financial) incentives to encourage digital services.
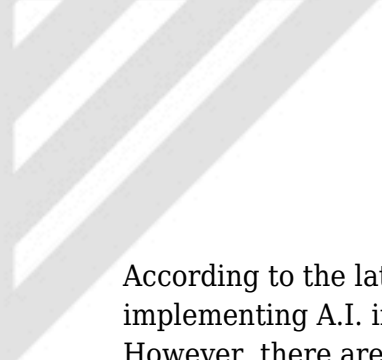
27. **To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?**

   The Swiss legal system has no specific regulation restricting the development of A.I.. In Switzerland, the use of A.I., machine learning and big data continues to increase. It is a fact that digitalisation plays a key role in our daily life and indirectly holds pressure on all the economic stakeholders to follow development.

   A.I. as a whole raises a lot of questions. Therefore, in Switzerland different institutions are conducting studies to answer questions regarding topics such as ethics or the risks and opportunities of A.I. innovation.

   In addition, the Swiss federal government funded research programs on the effective and appropriate use of big data and has incorporated a new federal working group specialized in A.I..

According to the latest A.I. research, the majority of companies are not yet prepared for implementing A.I. into their businesses nor do they know how to maximise the use of A.I.. However, there are some leading tech/telecom companies headquartered in Switzerland that have already started implementing and developing their own A.I..

For example, a leading Swiss telecom company is using chatbots in its customer support service and is offering support for other businesses to help implementing the use of A.I. in order to maximise income and respond to market demand.

Moreover, many companies already use intelligent wearables in order to help facilitate their employees' work and improve their results.

Hence, from a pragmatic point of view, the use of A.I. is trending, whereas from a regulatory perspective there are still many questions left unanswered.