The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Switzerland: Technology

This country-specific Q&A provides an overview to technology laws and regulations relevant in Switzerland.

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the merger control regime.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Lenz & Staehelin

The Legal 500

Dr. Lukas Morscher, Partner

lukas.morscher@lenzstaehelin.com

The Legal 500

Stefan Bürge, Associate

stefan.buerge@lenzstaehelin.com

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

Communications networks and services are regulated on the federal level, with the main source of law being the Federal Act on Telecommunications of 30 April 1997, as amended (TCA). The TCA governs any transmission of information by means of telecommunications techniques, except for television and radio program services. Further sources of law include the Federal Ordinance on Telecommunications Services of 9 March 2007, as amended (OTS), and the Federal Ordinance on Telecommunications Installations of 25 November 2015, as amended (TIO). As regards electronic communications equipment, Swiss requirements are largely in line with international and particularly European standards. The Federal Council can adopt technical regulations on telecommunications installations, particularly basic technical requirements for telecommunications, evaluation, certification or declaration of conformity. OFCOM regularly designates

technical standards. Compliance with these standards fulfils the basic requirements set out by the Federal Council. The standards are further explained in the TIO and the corresponding ordinance by OFCOM.

The telecommunications law framework applies to telecommunication service providers (TSPs), which are providers of services qualifying as telecommunication services. The TCA defines TSPs as services transmitting information for third parties using telecommunications techniques, which include the sending or receiving of information by wire, cable or radio using electrical, magnetic, optical or other electromagnetic signals.

There are two regulatory agencies in the telecommunications sector: the Federal Communications Commission (ComCom) and the Federal Office of Communications (OFCOM) (see Question 2 below). Fixed line and mobile telephony/satellite services are regulated by the TCA and its implementing ordinances. As regards fixed line services, no license is required. Rather, TSPs must (only) notify OFCOM of the intention to operate electronic communications networks or provide respective services. However, ComCom awards one or more universal service licenses to TSPs to ensure that universal service is guaranteed for the whole population of Switzerland in all parts of the country. TSPs offering mobile telephony and satellite services require a license as they make use of the radio frequency system. Generally, ComCom grants these licenses following an open invitation to tender.. ComCom is currently preparing the allocation of new mobile radio frequencies in the second half of 2018. These frequencies can be used as of 2019. Providers of voice over internet protocol (VoIP) services remain unregulated if they provide online services only, without transmitting data using telecommunications techniques. If the provider qualifies as a TSP (e.g. as a VoIP customer can also be reached by way of a fixed line telephone number as part of the public switched telephone network), the TCA applies. However, ComCom does not require such VoIP providers to fulfil all obligations the TCA imposes on regular TSPs; for example, they are under no duty to enable free carrier pre-selection (since there is no close link that needs to be broken between a network and a service operator) or the identification of the caller’s location in the case of emergency calls (which would be technically difficult to establish).

2. Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?

There are two regulatory agencies for the provision of communications-related services:

The Federal Communications Commission (ComCom) is the independent regulatory authority for the telecommunications market. Established by the TCA, it consists of seven members nominated by the Federal Council. ComCom is not subject to any Federal Council or Department directives. It is independent of the administrative authorities and has its own secretariat. ComCom’s responsibilities include, among other things, granting licenses for use of the radio frequency spectrum, awarding universal service licences, laying down the access conditions (unbundling, interconnection, leased lines etc.) when service

providers fail to reach an agreement, approving national numbering plans, fixing the terms of application of number portability/carrier selection and rendering decisions about supervisory measures and administrative sanctions.

The Federal Office of Communications (OFCOM) handles questions related to telecommunications and broadcasting (radio and television). OFCOM prepares the decisions of the Swiss government (Federal Council), the Swiss Federal Department for the Environment, Transport, Energy and Communications (DETEC) and the Swiss Federal Communications Commission (ComCom). OFCOM also serves as a point of contact for and coordinates international activities as regards Switzerland's position as an innovative location for business and research. OFCOM fulfils all regulatory tasks as regards telecommunications services and is, among other things, responsible for granting licences to all providers of fixed network services (without the tender procedure), the enforcement of the TSPs' obligation to register and the management of the frequency spectrum.

3. Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?

Generally, no restrictions apply to operators not domiciled in Switzerland or companies owning interests in the electronic communications market in Switzerland. However, subject to any international obligations to the contrary, ComCom may refuse to grant a license to use the radio frequency spectrum to foreign-incorporated companies unless reciprocal rights are granted to Swiss companies under the relevant foreign laws. Foreign TSPs obtaining contractual access to the network services of a TSP in Switzerland enter the market as Mobile Virtual Network Operators (MVNOs). MVNOs do not need an operation licence as their network is based on the transmission frequencies of the licenced operators. In Switzerland, there are three suppliers of mobile network infrastructure and several MVNOs.

4. Are there any regulations covering interconnection between operators? If so are these different for operators with market power?

As regards fixed line services, TSPs with a dominant position in the market must give other providers access to their facilities (technical co-use of locations related to network access) and services. They must provide access in a transparent and non-discriminatory manner and at reasonable prices including, among other things, as regards fully unbundled access to the local loop, rebilling for fixed network local loops, interconnection, access to leased lines and cable ducts (provided they have sufficient capacity). If two providers do not agree on the access conditions, one party can request that ComCom decides. Providers of services forming part of the universal service (such as mobile and fixed line services) must ensure that communication is possible between all users of these services and networks (interoperability). The

provisions for fixed line services also apply to mobile services providers. However, in practice only interconnection is relevant to mobile services, meaning that mobile services providers must ensure interoperability between each other and with providers of fixed line networks.

Dominant providers are subject to the Federal Act on Cartels and other Restraints of Competition (LCart) and the Federal Act on Price Surveillance, and may have limits imposed on their freedom to determine prices.

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

The TCA aims to ensure pricing transparency and the protection of users of communications services from abuse associated with value-added services. Hence, providers of telecommunications services must guarantee the transparency of prices for subscribers. Services of TSPs are also within the scope of the Price Notification Ordinance of 11 December 1978, as amended, meaning that the overall price of a telecommunication service must be given in Swiss francs and that price lists and catalogues must be readily accessible. The TCA also aims to protect users of communications services from unfair mass advertising: Spamming is prohibited under the Unfair Competition Act of 1 April 2007, as amended. The sender of mass advertisements submitted by means of telecommunications (such as e-mail, SMS, fax or automated telephone systems, but not physical mail) must seek the data subject's prior consent to such advertisement. TSPs must take measures against unfair mass advertisement and protect their customers from receiving it. For this purpose, they may intervene in user traffic and disconnect customers from the telecommunication network who send or forward mass advertising.

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

Computer software is protected under the Federal Act on Copyright and Related Rights of 9 October 1992, as amended (COPA). Copyrights generally vest in the author (i.e., the natural person that created a copyrightable work). In contrast, commercial exploitation rights in software developed by an employee in the course of employment vest in the employer. The owner of such rights is entitled to solely decide as regards the adaptation, reproduction, distribution, communication, broadcasting and other ways to commercialize or dispose of the computer software. The Federal Act against Unfair Competition of 19 December 1986, as amended (UCA), protects marketable work results (such as computer software) against technical reproduction performed without commensurate effort by the reproducing party.

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

Data/databases may be protected under COPA as collective works to the extent they qualify as original creations with individual character with respect to their selection and arrangement. Unlike EU law, Swiss law does not provide for general protection of databases by way of a right of its own (sui generis right) in favour of the creator. If databases do not reach the threshold of copyright protection as collective works, the economic effort to compile such database is generally not protected in Switzerland. In contrast, the UCA protects marketable work results against technical reproduction performed without commensurate effort by the reproducing party (see Question 6).

8. What key protections exist for personal data?

Switzerland has dedicated data protection laws. The Federal Data Protection Act (DPA) of 19 June 1992, as amended (DPA), and the Ordinance to the Federal Act on Data Protection of 14 June 1993, as amended (DPO), govern the processing of what in Switzerland is referred to as "personal data" by private parties or federal bodies. Several other federal laws contain provisions on data protection, which further address the collection and processing of personal data, in particular as regards the processing of personal data in regulated industries. As regards the telecommunications industry, the TCA regulates the use of cookies. As a general principle, personal information must always be processed (this includes collection and usage) lawfully. Such 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 information and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection) or non-compliance with these general principles is justified (e.g. by the data subject's voluntary informed consent or by law). The disclosure of personal information to third parties is generally lawful under the same conditions.

Switzerland is a member state to certain international treaties regarding data protection, such as the 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 (Convention ETS 108) and its additional protocol of 8 November 2001.

The Data Protection Act (DPA) is currently undergoing revision and a draft for the revised DPA has been published in September 2017. However, the draft is still subject to parliamentary debate and therefore the final wording of the revised DPA remains uncertain. The Swiss parliament has decided to divide the ongoing revision into two parts as follows:

- The first part includes the revision of only those provisions of the DPA which are required due to the implementation of Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities

for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data. This Directive must be implemented by Switzerland as it forms part of the Schengen acquis. The scope of the Directive is limited to the processing of personal data by competent authorities for aforementioned purposes. Accordingly, it only imposes additional obligations on authorities conducting such processing as a controller and natural or legal persons processing personal data as a processor on behalf of such an authority.

- The second part of the DPA revision will include the revision of those DPA provisions necessary to uphold the EU adequacy decision for Switzerland and, accordingly, will contain an equivalent of many of the provisions introduced in the EU through the GDPR. This second part will be taken up subsequently and the respective timing remains unknown (although it is currently not expected that the second part of the revision will enter into force before late 2019 or 2020).

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

Personal data may only be transferred outside Switzerland if the privacy of the data subject is not seriously endangered, in particular due to the absence of legislation that guarantees adequate protection in the jurisdiction where the recipient resides. The Federal Data Protection and Information Commissioner (FDPIC) has published a list of jurisdictions that provide adequate data protection (https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html). The EEA countries and Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay are generally considered to provide an adequate level of data protection as regards personal information of individuals (however, many do not as regards personal information of legal entities), while the laws of all other jurisdictions do not provide adequate data protection.

As regards the US, Switzerland and the US in February 2017 agreed on the Swiss-US Privacy Shield as a new framework for the transfer of personal data from Switzerland to the US, thereby replacing the US-Swiss Safe Harbor Framework. US companies processing personal data may self-certify to the Swiss-US Privacy Shield with the US Department of Commerce and thus publicly commit to comply with the new framework. Switzerland acknowledges that the level of protection of personal data for such certified US companies is adequate. As a result, Swiss companies are able to transfer personal data to those US business partners without the need to procure the consent of each data subject or to put additional measures in place.

In the absence of legislation that guarantees adequate protection, personal information may only be transferred outside Switzerland if sufficient safeguards, in particular 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 the performance of a contract (and the personal information 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 (further justifications apply). In practice, data transfer agreements or data transfer clauses (i.e. binding corporate rules) are regularly used to ensure an adequate level of protection in cross-border data flows within the same legal person or company or between legal persons or companies that are under the same management. It is the responsibility of the data transferor to ensure that an agreement is concluded that sufficiently protects the rights of the data subjects and to notify such agreements to the FDPIC. The FDPIC provides a model data transfer agreement which can be accessed on its website. The model data transfer agreement is based on Swiss law and reflects to a large extent the standard contractual clauses of the European Commission for data transfers.

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

Private persons are liable to a fine of up to CHF 10,000 for wilfully failing to provide information as regards safeguards in the case of cross-border data transfers or to notify data collections (or in so doing wilfully providing false information) or for wilfully providing the FDPIC with false information in the course of an investigation or for refusing to cooperate. On complaint, the wilful provision of false or incomplete information to data subjects who exercise their right of information or when collecting sensitive personal information of personality profiles, including the wilful failure to inform data subjects as required pursuant to the DPA, is sanctioned by a fine of up to CHF 10,000.

The preliminary draft of the revised DPA (see Question 7) imposes fines of up to CHF 250,000 for the breach of the obligations set forth above and further obligations set forth in the DPA. Further, wilful breach of professional secrecy shall be punishable by imprisonment of up to three years or monetary penalty. This new sanction will not be limited to the usual bearers of professional secrets but extend to any profession for which protection of confidentiality is essential.

11. Are there any restrictions applicable to cloud-based services?

There are no restrictions specifically applicable to cloud services. In general, personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity. Further, the use of cloud services constitutes an outsourced processing service if the personal data is not encrypted during its storage in the cloud and, in case the servers of the cloud are located outside Switzerland and the personal data is not encrypted during its transfer and storage, an international transfer of personal data (see Question 8). FDPIC has issued a non-binding guide outlining the general risks and data protection requirements of using cloud

services (https://www.edoeb.admin.ch/edoeb/en/home/data-protection/Internet_und_Computer/cloud-computing/guide-to-cloud-computing.html). Specific rules may apply in regulated markets (e.g. Circular 2018/3 relating to outsourcing issued by the Swiss Financial Market Supervisory Authority (FINMA) applies to banks and securities dealers organised under Swiss law, including Swiss branches of foreign banks and securities dealers subject to FINMA supervision).

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

The Code of Obligations sets out the principles governing e-signatures and refers to the Electronic Signatures Act of 18 March 2016, as amended (ESA), for the technical details, which in turn refers to its respective ordinance. An electronic signature is defined as electronic data which is joined or linked logically to other electronic data and which serves to verify such other data. The ESA distinguishes three levels of e-signatures: regular e-signatures, advanced e-signatures and authenticated e-signatures. The authenticated e-signature is deemed equivalent to a handwritten signature and can only be obtained from a recognised authority. A list of all such authorities 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 e-signatures are only available for natural persons, not for legal entities.

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

In a direct outsourcing setup in the private sector, the outsourcing agreement between the customer and the supplier is authoritative as regards the transfer (if any) of employees, assets or third party contracts. Where a transferor transfers a business (or part thereof) to a transferee, the employment agreements and all rights and obligations derived from them transfer by operation of law from the transferor to the transferee at the date of transfer of the business, unless the employee refuses this transfer. According to court practice and doctrine, "business" is any permanent self-contained organisational unit which is economically autonomous, and "part of a business" is an organisational unit which lacks economic autonomy. While the outsourcing supplier must generally use relevant customer assets, this can be achieved by granting a right to use the assets (on a shared or exclusive basis) rather than an outright transfer. Retaining title to an asset, license or contract can give the customer better protection in case of termination of the outsourcing agreement. A written assignment is usually sufficient to transfer movable property for evidential purposes. Transfer of title to real property must be made by public deed and, in

many cases (depending on the nature of the title involved) requires registration. Where the asset is a lease, the landlord's consent is required.

The transfer of key contracts should be agreed in writing based on analysis whether such transfer requires the counterparty's consent (as is usually the case; e.g. generally in case of IP licenses) or not (where approval of the transfer is already given in the contract). Absent or pending consent of the counterparty to the transfer (and subject to the terms of the contract prohibiting this), the customer may retain ownership of the contract and allow the supplier to perform the contract in relation to the counterparty as an agent of the customer.

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

There are no specific rules as regards A.I. functionality under Swiss law. From a civil law perspective, technology-neutral general Swiss liability law is applied, with the main sources of law being the Code of Obligations as regards fault-based and contractual liability as well as the Federal Road Traffic Act of 19 December 1958, as amended (RTA), and the Federal Law on Product Liability of 18 June1993, as amended (PLA), which address strict liability. The decisive factor for any liability is to whom the unlawful conduct is attributable. Only individuals or legal entities may be liable while a liability for a machine or A.I. functionality is excluded, meaning that the liability for the operation of autonomous systems (including A.I. functionalities) must always be based on the act or omission of a person, irrespective of an integrated software’s capability to amend the underlying software code. A similar logic applies from a criminal law perspective: Only individuals (and not machines) can be primarily criminally liable pursuant to the Swiss Criminal Code of 21 December 1937, as amended (SCC), meaning that an individual must have caused (by act or omission) an unlawful offense (e.g. a bodily injury or damage to an object) wilfully or negligently. A subsidiary liability for legal entities may apply if it is not possible to attribute an act or omission to an individual due to the inadequate organisation of such legal entity. Sanctions of up to CHF 5 mio. may be imposed for a felony or misdemeanour attributed to such legal entity.

15. What key laws exist in terms of obligations as to the maintenance of cyber security?

No cross-sector cybersecurity rules as regards minimum security requirements have been adopted in Switzerland. Sector-specific rules and regulator guidance are applicable. In general, personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity (see Question 10). While adherence to international standards relating to cybersecurity (e.g. ISO 27001 2013) is not mandatory in Switzerland, such standards

are considered as a relevant tool for assessing compliance with best practices. As regards data security, the FDPIC has become active only in a limited number of cases. Under the TCA, OFCOM is responsible for implementing the administrative and technical requirements pertaining to the security and availability of telecommunications services, which includes notifying the regulator in the event of security incidents. Specific rules apply to providers of financial markets infrastructure, including, among other things, to ensure the availability, confidentiality and integrity of data as well as business continuity.

16. What key laws exist in terms of the criminality of hacking/DDOS attacks?

Hacking and DDOS attacks are criminally sanctioned in Switzerland pursuant to the SCC. More generally, the unauthorised obtaining of data (including by unlawfully gaining access to a data processing system), damage to data, computer fraud, breach of secrecy or privacy through the use of an image-carrying device, obtaining personal data without authorisation, industrial espionage and the breach of the postal or telecoms secrecy are all criminally punishable with sanctions ranging from monetary penalties to imprisonment of up to three years.

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

Based on its general technology neutrality, the Swiss regulatory framework allows for ample regulatory latitude and room for development for technology driven business models and companies, including compared with other jurisdictions. Specific areas of presumed legal development includes the legal classification of virtual currencies as digital objects and the evidentiary value of confirmations provided for digitised assets and the transfer thereof by means of distributed ledger technology (public faith in blockchain entries).

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

Legal ownership of digital objects is not established under Swiss law and ownership generally requires an object to be tangible for the owner to be in a position to claim legal title and exercise factual control over such object as property. Digital information is not tangible and can therefore, according to current Swiss law, not be subject to legal ownership. However, "ownership" of digital objects is often allocated in contracts, as between the parties (i.e. with effect for the parties of the respective agreement only), to one of the contracting parties. Similarly, there is as of yet no public faith in the digital records of the assets and

of the transfer as registered by means of public ledger technology (blockchain). Acknowledging such public faith will require legislative changes. A working group led by the Federal Department of Finance has been mandated to provide suggestions on recommended further steps, including with respect to appropriate legislative changes. The working group is expected to report to the Federal Council by the end of 2018.

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

The Swiss regulatory framework encourages digital services, in particular due to the technology-neutral approach of the legislator, thereby allowing for ample room for development for technology driven business models and companies. Hence, there are generally no regulation-induced impediments to technology innovation under current law. Government authorities periodically review developments in technology and generally emphasize the importance of making use of technological progress. Considerable efforts are undertaken to further facilitate lower market entry barriers for technology-driven business models.

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

There are currently no specific rules as regards A.I. functionality under Swiss law and we are not aware of any intentions of the legislator to enact such rules. While government authorities periodically review respective practical developments, it is emphasized that regulation should be technology-neutral. The Federal Council has repeatedly stated and it is widely held in the legal community that A.I. specific legislation is neither required nor desirable in order to allow for the regulatory latitude and room for development required for technology driven business models and companies.