Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

TMT

Switzerland
Lenz & Staehelin

chambers.com

2019

Law and Practice

Contributed by Lenz & Staehelin

Contents

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

Authors

Lukas Morscher is the head of TMT and outsourcing and is a partner with a wealth of experience in outsourcing (IT outsourcing, business process outsourcing and transactions), TMT, corporate and M&A, internet and e-commerce, data protection and privacy, FinTech, digitisation and industry 4.0. Lukas is a member of the SwissICT, the Swiss Internet Industry Association, Schweizer Forum für Kommunikationsrecht and the International Technology Law Association.

Stefan Bürge is an associate who specialises in technology, IP, licensing and distribution, media and telecoms, data protection and privacy, investigations, unfair competition, advertising, commercial and contracts. He is a member of the International Technology Law Association, the Swiss Finance + Technology Association, the International Association for the Protection of Intellectual Property, the Licensing Executives Society, the International Trademark Association and the Swiss Forum for Communications Law.

Nadja Flühler is an associate who has experience in issues related to outsourcing (IT outsourcing, business process outsourcing and transactions), TMT, corporate and M&A, internet and e-commerce, data protection and privacy, FinTech, digitisation and industry 4.0. She is a member of the International Technology Law Association.

1. Cloud Computing

1.1 Laws and Regulations

Under Swiss law, there are no rules specifically applicable to cloud computing. There are, in particular, no regulations prohibiting, restricting or otherwise governing cloud computing. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to cloud computing.

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. The use of cloud services may qualify as an outsourced processing service and, in cases where the servers of the cloud are located outside Switzerland and the personal data is not fully encrypted during transfer and storage, an international transfer of personal data (see **6. Key Data Protection Principles**, below). The Federal Data Protection and Information Commissioner (FDPIC) has issued a non-binding guideline setting out the general risks and data protection requirements with respect to the use of cloud services.

The Federal Act on the Surveillance of Mail and Telecommunication Traffic of 18 March 2016, as amended (BÜPF), applies to providers of derived communication services, which includes cloud service providers. Where telecommunication services are involved in criminal investigations, service providers are obliged to tolerate surveillance measures and to provide access to their data processing systems upon

order by competent authorities. Specific rules may apply in regulated markets, such as the banking sector (eg, 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).

In the event a customer of a cloud services provider is subject to compliance requirements as set out above or respective contractual obligations towards a third party, applicable obligations have to be set out in writing in the contracts with the cloud services provider. This applies, in particular, to compliance with data protection regulations as imposed on the customers of cloud services providers.

1.2 Regulations in Specific Industries

See **1.1 Laws and Regulations**.

1.3 Processing of Personal Data

See **1.1 Laws and Regulations**.

2. Blockchain

2.1 Risk and Liability

In Switzerland, there is no specific regulation in relation to Distributed Ledger Technology (DLT) or blockchain. The Swiss legislature strives to keep laws technology-neutral, thus the general rules apply, including as regards risks, liability, intellectual property, anti-money laundering and data privacy. Switzerland has a suitable proven and balanced legal framework; hence, only limited and targeted adjustments as regards DLT/blockchain applications are currently contemplated. While the Swiss legislature is aware that the possibilities offered by DLT/blockchain go far beyond the application to such alternative financings, there is a legislative focus on the financial sector. As regards ICOs, the FINMA published the 'ICO Guidelines for enquiries regarding the regulatory framework for initial coin offerings' of 16 February 2018 and clarified that tokens do not constitute a separate regulatory category. The existence of a token therefore has no legal meaning of its own. FINMA's approach is therefore based, among others, on the existence of securities traded in the form of tokens.

Anti-money Laundering

Transactions in cryptocurrencies may be carried out on an anonymous basis and related money laundering risks are accentuated by the speed and mobility of the transactions made possible by the underlying technology. The Know Your Customer (KYC) principle is the cornerstone of the Anti-money laundering (AML) and combating the financing of terrorism (CFT) due diligence requirements that are generally imposed on financial institutions whose AML/CFT legislation is aligned with international standards. KYC requires that financial institutions duly identify (and verify) their contracting parties (ie, customers) and the beneficial owners (namely when their contracting parties are not natural persons) of such assets as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets (ie, paper trail) and allows the identification of money laundering and financing of terrorism indicia. With respect to DLT/blockchain applications, one of the challenges is that KYC and other AML/CFT requirements are designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed by each jurisdiction at the level of financial intermediaries operating on its territory (ie, acting as 'gatekeepers'). By contrast, virtual currency payment products and services rely on a set of decentralised cross-border virtual protocols and infrastructure elements, neither of which has a sufficient degree of control over or access to the underlying value (asset) and/or information, meaning that that identifying a touch-point for implementing and enforcing compliance with AML/CFT requirements is challenging.

Swiss AML legislation does not provide for a definition of virtual currencies. However, since the revision of the Swiss Financial Market Supervisory Authority (FINMA) AML Ordinance in 2015, exchange activities in relation to virtual currencies, such as money transmitting (ie, money transmission with a conversion of virtual currencies between two parties), are clearly subject to general AML rules. Further, the purchase and sale of convertible virtual currencies on a commercial basis and the operation of trading platforms to transfer money or convertible virtual currencies from the users of a platform to other users are subject to Swiss AML rules. Before commencing operations, providers of such services must either become a member of a self-regulatory organisation or apply to FINMA for a licence to operate as a directly supervised financial intermediary.

Working Group Blockchain/ICO

In January 2018, the State Secretariat for International Finance (SIF) together with the Federal Office of Justice and FINMA set up a working group on blockchain and ICOs. Its ongoing task is to identify specific legislative need for action for financial applications of blockchain technology and to evaluate the corresponding legal framework. Based on a broad consultation process, the Federal Council has published a report in December 2018 which concluded that existing legislation is generally well suited to enable DLT/blockchain applications in the financial industry and that there is only limited need for legislative action to strengthen the existing legal framework (including, among other things, civil law amendments to strengthen legal certainty in the context of transferring rights by means of digital registers and a right of separation for digital assets in case of insolvency). The Federal Office of Justice has been mandated to develop such limited legislative proposal.

2.2 Intellectual Property
See **2.1 Risk and Liability**.

2.3 Data Privacy
See **2.1 Risk and Liability**.

2.4 Service Levels
See **2.1 Risk and Liability**.

2.5 Jurisdictional Issues
See **2.1 Risk and Liability**.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Big Data
Big data, machine learning and artificial intelligence offer new opportunities to develop social or scientific knowledge and can be the basis for further form of value creation by companies. In general, there is no cross-sector regulation in Switzerland regarding big data, machine learning and artificial intelligence. As regards the processing of personal data, the right to privacy and the protection of personal data must be safeguarded (see **6 Key Data Protection Principles**, below). While government authorities periodically review developments as regards big data, machine learning and artificial intelligence, it is acknowledged that any regulation should be technology-neutral in order to accommodate new developments within the existing legal and regulatory framework. This enables businesses located in Switzerland to make optimal use of upcoming technologies and advancements and to efficiently adapt their business models and processes as required or desired.

The Federal Council set up a federal working group on artificial intelligence under the direction of the State Secretariat for Education, Research and Innovation (SERI), which facilitates the exchange of knowledge and opinions and the co-ordination of Switzerland's positions in international bodies. It is expected that it will in autumn 2019 submit to the Federal Council an overview of existing measures, an assessment of possible fields of action and considerations on the transparent and responsible use of artificial intelligence.

3.2 Machine Learning
See **3.1 Big Data**.

3.3 Artificial Intelligence
See **3.1 Big Data**.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions Affecting a Projects' Scope
The Internet of things (IoT) refers to objects and devices which are connected to a network such as the Internet and which use the network to communicate with each other or make information available. The connecting device may be a modem, network-attached storage (NAS), a webcam, intelligent light switches or smart TVs connected to an internal network or the Internet. The Swiss regulatory framework encourages digital services – in particular, due to the technology-neutral approach of the 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 emphasise the importance of making use of technological progress. Considerable efforts are undertaken to further facilitate lower market entry barriers for technology-driven business models.

As more and more intelligent devices are connected to the Internet, not only the number of communications participants involved has grown but also the number of vulnerable devices that may be misused by hackers increases (eg, for sending spam e-mails). Such devices need to be adequately protected (eg, by using individual password or restricted access) and respective software has to be kept updated. Between objects and devices that communicate with each other, typically large amounts of information and data are exchanged. This may also have an impact on the protection of personal data and the general rules of data protection apply. Any data subject is protected from its personal data being processed in a way that is not in compliance with the law or used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification applies (see **6 Key Data Protection Principles**, below).

To protect critical information and communication infrastructure in Switzerland, the Federal Council has commissioned the Reporting and Analysis Centre for Information Assurance (MELANI). To prevent devices within the IoT from being misused by hackers, MELANI recommends preventive measures on its website. These measures include, among others, the establishment of a separate network segment for devices connected with the Internet and devices connected to personal data, restricting access from the Internet to the device, using protocols allowing only encrypted connection and using complex passwords and second factor authentication.

5. Challenges with IT Service Agreements

5.1 Specific Features

Under Swiss law, there is no specific regulation in relation to IT service agreements. However, there are statutes governing the general outsourcing of services to (IT) providers in certain industries (eg, the financial industry, telecommunications and the public sector). As regards financial services there is sector-specific regulation. In particular, the outsourcing of business areas (infrastructure or business processes) by Swiss financial institutions is subject to:

- Article 47 of the Swiss Federal Banking Act of 8 November 1934, as amended (Banking Act), on banking secrecy, protects customer-related data from disclosure to third parties and applies to all banking institutions in Switzerland. Any disclosure of non-encrypted data to a supplier is only allowed with the express consent of each banking customer. Consent can be given under the bank's general terms of business if they are made an integral part of the contract between the bank and its customers. The Banking Act does not prohibit the transfer of encrypted data (where the supplier cannot identify individual customers).
- Circular 2018/3 relating to outsourcing (Outsourcing Circular) issued on 21 September 2017 by the Swiss Financial Market Supervisory Authority (FINMA, the supervisory authority for banks, insurers, reinsurers, stock exchanges, securities dealers, collective investment schemes and audit firms) applies to banks, securities dealers and insurers organised under Swiss law, including Swiss branches of foreign banks, securities dealers and insurers which are subject to FINMA supervision. Before outsourcing significant business areas, these institutions must comply with the detailed measures set out in the Outsourcing Circular, including the obligation to keep an inventory of all outsourced services (which must include proper descriptions of the outsourced function, the name of the service provider and any subcontractors, the service recipient and the person or department responsible within the company); careful selection, instruction and control of the supplier; and conclusion of a written contract with the supplier setting out, among others, security and business continuity requirements and audit and inspection rights.

The customer remains responsible for the outsourced business areas, so it must ensure their proper supervision. Swiss banks, securities dealers and insurers must also consider that outsourcings to independent service providers are generally considered to increase operational risks and therefore lead to additional capital requirements for them.

The outsourcing of services to an IT service provider may also impact the protection of personal data. Any data subject is protected from its personal data being processed in a way that is not in compliance with the law or used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification applies (see **6 Key Data Protection Principles**, below). However, personal data may be given to outsourcing suppliers based on a contract or statutory law if the customer ensures that the supplier will only process data in a way that the customer is itself entitled to, and that the supplier will comply with the applicable data security standards, and if no statutory or contractual secrecy obligations prohibit this data processing. As the customer remains liable towards the data subject for the compliant handling of personal data by the supplier, and reflecting the growing importance of data protection, there is a tendency not to apply a liability cap for breaches of data protection or other regulatory requirements in outsourcing agreements. This is particularly the case when sensitive data such as business secrets or bank customer data are involved.

5.2 Rules and Restrictions

See **5.1 Specific Features**.

6. Key Data Protection Principles

6.1 Core Rules Regarding Data Protection

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. Processing of personal data by cantonal authorities (cantons are the Swiss states) is subject to separate state legislation. In addition, several other federal laws contain provisions on data protection, which further address the collection and processing of personal data, especially as regards the processing of personal data in regulated industries (such as financial markets and telecommunications):

- the Swiss Federal Code of Obligations (Code of Obligations) sets forth restrictions on the processing of employee data, and Ordinance 3 to the Swiss Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer;
- the Swiss Federal Telecommunication Act (Telecommunication Act) regulates the use of cookies.
- the Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as e-mail and text messages;
- statutory secrecy obligations, such as banking secrecy (set forth in the Swiss Federal Banking Act (Banking Act)), securities dealer secrecy (set forth in the Swiss Federal Stock Exchange and Securities Dealer Act (Stock Exchange Act)), financial market infrastructure secrecy

(set forth in the Swiss Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (the Financial Market Infrastructure Act)) and telecommunications secrecy (set forth in the Telecommunication Act) apply in addition to the DPA;
- the Banking Act, the Stock Exchange Act and the Swiss Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector stipulate specific duties to disclose information;
- the Swiss Federal Act regarding Research on Humans, the Swiss Federal Act on Human Genetic Testing and the Swiss Federal Ordinance on Health Insurance set out specific requirements for the processing of health-related data.

The DPA and DPO apply to the processing of any data relating to an identified or identifiable person, irrespective of its form (ie to personal data pertaining to natural persons (individuals) and personal data pertaining to legal entities (companies)). A person is identifiable if a third party having access to the data on the person is able to identify such person with reasonable efforts. Pursuant to the DPA 'sensitive personal data' and 'personality profiles' are to be considered as special categories of personal data that are subject to stricter processing conditions. Sensitive personal data is data on:

- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or racial origin;
- social security measures; and
- administrative or criminal proceedings and sanctions.

A personality profile is a collection of personal data that permits an assessment of essential characteristics of the personality of a natural person.

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 (eg, 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.

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. The countries of the European Economic Area 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 data relating to individuals (however, many do not as regards personal data relating to legal entities), while the laws of all other jurisdictions do not provide adequate data protection. As regards the USA, Switzerland and the USA in February 2017 agreed on the Swiss–US Privacy Shield as a new framework for the transfer of personal data from Switzerland to the USA, 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 data may only be transferred outside Switzerland if, inter alia, sufficient safeguards (in particular, standard contractual clauses) ensure an adequate level of protection abroad, the data subject has consented in the specific case, the processing is directly connected with the conclusion or 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 (ie binding corporate rules). In practice, in order to ensure an adequate level or data protection, data transfer agreements or data transfer clauses (ie binding corporate rules) are regularly used. It is the responsibility of the data transferor to ensure that an agreement sufficiently protecting the rights of the data subjects is concluded. The FDPIC 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. The FDPIC has to be notified of the use of such agreements accordingly. Further, in case of regular processing of particularly sensitive data or personality profiles, or regular disclosure of personal data to third parties (whereby group companies qualify as third parties within the meaning of the DPA), the respective data files must be registered with the Swiss Federal Data Protection and Information Commissioner (FDPIC). Such data files have to be registered prior to being established. However, there are exemptions from such registration duty; in particular, if the respective data is processed as a matter of law or in the case of a voluntary appointment of a data protection officer. A list of such business organisations who have appointed a data protection officer is publicly accessible on the FDPIC's website.

The appointment of a data protection officer is not mandatory in Switzerland. However, the registration of data collections is not required if the owner of a data collection has appointed a data protection officer that independently monitors data protection compliance within the owner's business organisation and maintains a list of data collections. The appointment of a data protection officer will only result in a release of the duty to register data collections if the Federal Data Protection and Information Commissioner (FDPIC) is notified of the appointment of a data protection officer. A list of such business organisations who have appointed a data protection officer is publicly accessible on the FDPIC's website. The data protection officer has two main duties. First, the data protection officer audits the processing of PII within the organisation and recommends corrective measures if he or she finds that the data protection regulations have been violated. He or she must not only assess compliance of the data processing with the data protection requirements on specific occasions, but also periodically. The auditing involves an assessment of whether the processes and systems for data processing fulfil the data protection requirements, and whether these processes and systems are in fact enforced in practice. If the data protection officer takes note of a violation of data protection regulations, he or she must recommend corrective measures to the responsible persons within the organisation and advise them on how to avoid such violations in the future. The data protection officer does not, however, need to have direct instruction rights. Second, the data protection officer maintains a list of the data collections that would be subject to registration with the FDPIC. The list must be kept up to date. Unlike the data collections registered with the FDPIC, the internal data collections do not have to be maintained electronically nor must they be available online. However, they must be made available on request to the FDPIC and to data subjects.

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. Although Switzerland is not a member of the EU and, hence, has neither implemented the EU Data Protection Directive 95/46/EC nor is directly subject to the EU General Data Protection Regulation 2016/679 (GDPR), it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU. A revision of the DPA shall align the DPA with international rules on data protection in order to comply with the upcoming revision of Convention ETS 108 and the GDPR. This will allow Switzerland to uphold its status as a country adequately protecting personal data from an EU perspective, which allows for easier transfer of personal data from the EU and to ratify Convention ETS 108 of the Council of Europe.

The DPA is currently undergoing revision and the Swiss parliament has decided to divide the ongoing revision into two parts. The first part includes the revision of only those provisions of the DPA that 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 (the Directive). The 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 the 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. Thus, it is of less relevance for private companies.

The second part of the DPA revision (ie, the revision of those DPA provisions necessary to uphold the EU adequacy decision for Switzerland, such as provisions introduced in the EU through the GDPR) will be taken up subsequently and the respective timing remains unknown, although it is currently expected that the second part of the revision will enter into force around late 2019 or early 2020.

6.2 Distinction Between Companies/Individuals

See **6.1 Core Rules Regarding Data Protection**.

6.3 General Processing of Data

See **6.1 Core Rules Regarding Data Protection**.

6.4 Processing of Personal Data

See **6.1 Core Rules Regarding Data Protection**.

7. Monitoring & Limiting of Employee Use of Computer Resources

7.1 Employees' Restrictions on Computer Use

The processing of employee data by the employer, and in particular the monitoring of employees, is regulated by several Swiss law on different levels. In addition to the general provisions on data protection set out in the DPA and its implementing ordinances (see **6 Key Data Protection Principles**, above) the processing of employee personal data is further restricted by the Swiss Code of Obligations of 30 March 1911, as amended (CO). The employer may process personal data relating to an employee only to the extent that such data concerns the employee's suitability for his or her job or as necessary for the performance of the employment contract. In addition, pursuant to Swiss labour law, the monitoring and control of employees (such as monitoring and limiting the use of computer resources by an employer) is subject to certain further restrictions according to Arti-

cle 26 of Ordinance 3 to the Swiss Federal Act on Employment in Trade and Industry of 13 March 1964, as amended. Surveillance and control systems monitoring the employee behaviour at the workplace (Monitoring Systems), such as the examination or monitoring of an employee's office desk or systems – eg, e-mails, voice mail, fax and video recording – are prohibited if monitoring the employee's general behaviour is the sole or predominant purpose of such systems. The use of Monitoring Systems is, however, permissible where legitimate reasons apply and such use is proportionate (ie suitable, necessary and reasonable). In general, legitimate reasons are, among others, security measures, worktime control, quality and productivity control, improvement of organisation or planning of the work as well as reasons which are inherent to the nature of the employment itself.

8. Scope of Telecommunications Regime

8.1 Technologies within Local Telecommunications Rules

In Switzerland, the telecommunications sector is regulated at federal level. The main source of law is 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 programme 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. The Federal Office of Communications (OFCOM) regularly designates technical standards. Compliance with these standards fulfils the basic requirements set out by the Federal Council. 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.

In the telecommunications sector there are two regulatory agencies: the Federal Communications Commission (ComCom) and the OFCOM. Fixed line and mobile telephony/satellite services are regulated by the TCA and its implementing ordinances. As regards fixed line services, no licence 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 licences 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 licence as they make use of the radio frequency system. Generally, ComCom grants these licences following an open invitation to tender. 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 (eg, 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).

9. Audiovisual Services and Video channels

9.1 Main Requirements

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

The Federal Media Commission (FMEC) advises the Federal Council and the Federal Administration in relation to media issues. The Federal Radio and Television Act of 24 March 2006, as amended (RTVA), provides for an Independent Complaints Authority for Radio and Television, which deals with complaints that relate to the editorial programme and rules on disputes on denied access to a programme. In Switzerland, apart from the communications sector, regulation of the media sector is also dealt with at a federal level. The broadcasting, processing and reception of radio and television programme services are regulated by the RTVA, the Federal Ordinance on Radio and Television of 9 March 2007, as amended (RTVO), and related regulation.

Broadcasters of programme services are, in principle, required to obtain a licence. Broadcasters that neither request splitting revenue nor guaranteed wireless terrestrial distribution may operate their service without a licence. However, such broadcasters need to notify OFCOM. Also, broadcasters of programme services of minor editorial importance (such as programme services that can only be received by fewer than 1,000 people at the same time) do not fall under the scope of the RTVA and do not need a licence or registration. If the broadcaster of a radio programme service is granted a licence under the RTVA, it is at the same time granted a licence under the TCA for use of the frequency spectrum (no separate application is needed). Cable TV operators are under a duty to broadcast in the respective coverage area TV programme services of broadcasters that have been granted a licence. Licences are awarded by public tender. There are no rules specifically applicable to the operation of a video channel (such as YouTube channel). Since the Swiss legislature strives to keep laws technology-neutral the general rules apply to the operation of video channels. To be awarded a licence, the applicant must be able to fulfil the mandate, possess sound financial standing, be transparent regarding its owners, guaranteeing compliance with employment law regulations and the working conditions of the industry, the applicable law and in particular the obligations and conditions associated with the licence, maintain a separation of editorial and economic activity, and have registered offices in Switzerland.

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

Lenz & Staehelin
Brandschenkestrasse 24
CH-8027
Zurich

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

9.2 Online Video Channels

See **9.1 Main Requirements**.

10. Encryption Requirements

10.1 Legal Requirements Governing the Use of Encryption

In Switzerland, there is no specific regulation in relation to encryption. Technology, media and telecom providers are not directly required to use encryption technology. However, pursuant to the Federal Act on Data Protection of 19 June 1992, as amended (DPA), any information qualifying as personal data must be protected by appropriate technical and organisational measures against unauthorised processing, which in general includes encryption (see **6 Key Data Protection Principles**, above).

In particular, the personal data must be protected against unauthorised or accidental destruction; accidental loss; technical faults; forgery, theft or unlawful use; and unauthorised alteration, copying, access or other unauthorised processing. Hence, many providers rely on encryption technology when processing personal data. In this context data protection law provides for certification of products intended for processing of personal data. Manufacturers of data processing systems or programs as well as private persons or federal bodies that process personal data may submit their systems, procedures and organisation (which usually encompass encryption as means of data security) for evaluation by recognised (ie, accredited) independent certification organisations. However, the use of encryption technology does generally not exempt from compliance with general data protection rules.

In civil, criminal or public procedures authorities may compel parties to such proceedings, or even non-involved third parties, to disclose certain information in accordance with such parties' duty to prove or disprove disputed facts before the respective authority. This may include information that is stored in an encrypted format, in which case the party in question has to disclose the information in an unencrypted, readily accessible format. Available enforcement mechanisms depend on the type of procedure and the role the person concerned has in such procedure.

The use of encryption systems (such as public key infrastructures) is protected by criminal law pursuant to the Federal Criminal Code of 21 December 1937, as amended (CC). Any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his or her access is liable to imprisonment not exceeding three years or to a monetary penalty (Article 143bis para 2 CC). Simi-

larly, with respect to computer fraud, any person who by the incorrect, incomplete or unauthorised use of data (or in a similar way) influences the electronic or similar processing or transmission of data and as a result causes the transfer of financial assets is liable to imprisonment not exceeding five years (not exceeding ten years in case a commercial gain is intended) or to a monetary penalty (Article 147 CC).

10.2 Exemptions

See **10.1 Legal Requirements Governing the Use of Encryption**.