Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2023

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

Switzerland: Law & Practice
Lukas Morscher and Nadja Guberan-Flühler
Lenz & Staehelin

practiceguides.chambers.com

SWITZERLAND

Law and Practice

Contributed by:
Lukas Morscher and Nadja Guberan-Flühler
Lenz & Staehelin see p.18

Contents

1. Metaverse p.3
1.1 Laws and Regulations p.3

2. Digital Economy p.4
2.1 Key Challenges p.4

3. Cloud and Edge Computing p.5
3.1 Highly Regulated Industries and Data Protection p.5

4. Artificial Intelligence and Big Data p.9
4.1 Liability, Data Protection, IP and Fundamental Rights p.9

5. Internet of Things p.9
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.9

6. Audio-Visual Media Services p.10
6.1 Requirements and Authorisation Procedures p.10

7. Telecommunications p.12
7.1 Scope of Regulation and Pre-marketing Requirements p.12

8. Challenges with Technology Agreements p.13
8.1 Legal Framework Challenges p.13

9. Trust Services and Digital Entities p.16
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes p.16

1. Metaverse

1.1 Laws and Regulations

In Switzerland, there is no specific regulation in relation to the metaverse. 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. There are, however, existing regulations that are particularly relevant in the context of the metaverse.

Switzerland has a suitable, proven and balanced legal framework; hence, only limited and targeted adjustments as regards metaverse/distributed ledger technology (DLT)/blockchain applications are currently contemplated. While the Swiss legislature is aware that the possibilities offered by the metaverse/DLT/blockchain go far beyond their application to alternative financing, there is a legislative focus on the financial sector.

As regards the application of the existing regulations on initial coin offerings (ICOs), the Swiss Financial Market Supervisory Authority (FINMA) published corresponding guidelines on 16 February 2018. Generally, FINMA focuses on the economic function and purpose of the tokens, as well as whether they are tradeable or transferable, in order to classify the tokens broadly into three "archetypes":

- payment tokens (which include cryptocurrencies);
- utility tokens; and
- asset tokens.

The classification of the individual token impacts the applicable legal and regulatory framework–ie, tokens do not constitute a separate regulatory category. Since then, FINMA has issued further guidelines on money laundering on the blockchain and, most recently, also on stable coins.

In December 2018, the Swiss Federal Council published a report on the legal framework for blockchain and DLT in the financial sector, which noted that the Swiss legal framework is, in principle, well suited to deal with new technologies.

The DLT Act

In September 2020, parliament adopted the Federal Act on the Adaption of Federal Law to Developments in Distributed Ledger Technology (the "DLT Act"), with which various federal laws were adapted in order for Switzerland to continue to develop as a leading, innovative and sustainable location in the context of the metaverse and, in particular, for blockchain and DLT activity.

The amendments include:

- a civil law amendment aimed at increasing legal certainty regarding the transfer of DLT-based digital assets;
- the possibility of segregation of digital assets in the event of bankruptcy; and
- the introduction of a "DLT trading facility" (as a new authorisation category), which may offer trading, settlement and clearing services in relation to digital assets.

Overall, these legislative amendments are expected to increase market access to fintech companies working in the field of DLT/blockchain technologies by improving legal certainty and removing certain regulatory barriers. The provisions enabling the introduction of uncertificated register securities that are represented on a blockchain entered into force on 1 February 2021, and the remaining provisions of the DLT Act entered into force on 1 August 2021.

Anti-money Laundering

Transactions made within the context of the metaverse and particularly 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 where 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 (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, papertrail) and allows the identification of money laundering and financing of terrorism indicia.

With respect to the metaverse, including 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 the 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, none 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 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. Furthermore, 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.

Since DLT-trading facilities (the separate licence category introduced by the DLT Act as an amendment to the Financial Market Infrastructure Act (FMIA); see above) can carry out activities that qualify as financial intermediation under the Anti-Money Laundering Act (AMLA), they are to be included in the AMLA as specifically regulated financial intermediaries.

Data Protection

Personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is processed or stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity, including in the metaverse environment (see **3. Cloud and Edge Computing** regarding data protection principles).

2. Digital Economy

2.1 Key Challenges

Under Swiss law, there are no rules specifically applicable to the digital economy. There are, in particular, no regulations particularly regarding digital services, digital markets or content reg-

ulations. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to the digital economy (see also **1. Laws and Regulations** regarding the metaverse; **4. Artificial Intelligence and Big Data** and **9. Trust Services and Digital Entities**).

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud and Edge Computing

Under Swiss law, there are no rules specifically applicable to cloud and edge computing. There are, in particular, no regulations prohibiting, restricting or otherwise governing cloud and edge computing. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to cloud and edge 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, as an international transfer of personal data (see below). The Swiss 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 (*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs*, 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 FINMA, which applies to banks, insurers and securities firms organised under Swiss law, including Swiss branches of foreign banks, insurers and securities firms 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.

Data Protection Legislation

Switzerland has dedicated data protection laws. The Federal Data Protection Act 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 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 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 Act on Telecommunications of 30 April 1997, as amended (TCA), regulates the use of cookies.

The Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as email and text messages.

Statutory secrecy obligations, such as banking secrecy (set forth in the Banking Act), financial institutions secrecy (set forth in the Financial Institutions Act (FinIA)), financial market infrastructure secrecy (set forth in the FMIA) and telecommunications secrecy (set forth in the TCA) apply in addition to the DPA.

The Banking Act, the FinIA 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.

Personal 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 that 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 the 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 incompliance 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, if non-compliant 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.

Cross-Border Data Transfers

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 FDPIC has published a list of jurisdictions that provide adequate data protection. The countries of the EEA 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 data transfers to the USA, the Swiss-US Privacy Shield (which replaced the US-Swiss Safe Harbour Framework in 2017), under which Swiss companies were able to transfer personal data to their US business partners without the need to procure the consent of each data subject or to put additional measures in place, was declared invalid by the FDPIC in September 2020. The FDPIC concluded that although the Swiss-US Privacy Shield guarantees special protection rights for persons in Switzerland, it does not provide an adequate level of protection for data transfer from Switzerland to the USA pursuant to the DPA. As a result, Swiss companies can no longer rely on the Swiss-US Privacy Shield for the transfer of personal data from Switzerland to the USA without additional safeguards or justification (see below). Further, prior to any data transfer from Switzerland to the USA or any other country not providing adequate data protection, data controllers are advised to perform a so-called data transfer impact assessment, assessing the risks associated with such transfer. The FDPIC has taken note of the Trans-Atlantic Data Privacy Framework, which has been recently negotiated between the EU and the USA and is currently reviewing this new data privacy framework.

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 of 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 currently being revised by the FDPIC. The model data transfer agreement is based on Swiss law and reflects, to a large extent, the former version of the standard contractual clauses of the European Commission for data transfers (SCC).

The FDPIC recognises the new set of SCC, issued by the European Commission on 4 June 2021, for data transfers to countries not providing adequate data protection level, provided that

the necessary adaptations and amendments are made for use under Swiss data protection law. Since 1 January 2023, data transfers must be based on the new SCC or the revised model data transfer agreement once available (the old SCC as well as the model data transfer agreement may no longer be used for such transfers).

The FDPIC has to be notified of the use of such agreements accordingly. Furthermore, in the 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 FDPIC. The data files have to be registered prior to being established. However, there are exemptions from this 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 business organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website.

Data Protection Officers

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 FDPIC is notified of the appointment of a data protection officer. A list of business organisations that 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 personal data within the organisation and recommends corrective measures if they find that the data protection regulations have been violated. They 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 enforced in practice. If the data protection officer takes note of a violation of data protection regulations, they 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.

Swiss Alignment with International Data Protection Standards

Switzerland is a state party 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 Directive95/46/EC nor is directly subject to the EU General Data Protec-

tion 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.

The Swiss parliament recently adopted a revision of the DPA. The revision of the DPA aligns the DPA with international rules on data protection in order to comply with the revised 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 the ratification of Convention ETS 108.

The revised DPA largely follows the regime provided by the GDPR with some reliefs and very limited "Swiss finishes" (ie, rules that go beyond the requirements of the GDPR – most importantly, every country to which personal data is transferred to will have to be explicitly named). The revised DPA will enter into force on 1 September 2023.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Big data and artificial intelligence (AI) offer new opportunities to develop social or scientific knowledge and can be the basis for further forms of value creation by companies. In general, there is no cross-sector regulation in Switzerland regarding big data or AI. As regards the processing of personal data, the right to privacy and the protection of personal data must be safeguarded (see **3. Highly Regulated Industries and Data Protection** regarding data protection principles). While government authorities periodically review developments as regards big data and AI, 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 advances, and to efficiently adapt their business models and processes as required or desired.

The Federal Council has 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. Based on a report of SERI submitted to the Federal Council outlining existing measures, an assessment of possible fields of action and considerations on the transparent and responsible use of AI, the Federal Council concluded on 13 December 2019 that Switzerland is, in general, well suited to address AI applications, business models and challenges. Thus, there is no immediate need to adapt the existing legislative framework, subject to certain specific areas (such as mobility, security policy, education and research) in which, however, a multitude of measures have already been initiated to address corresponding challenges. Further, on 25 November 2020, the Federal Council adopted guidelines for dealing with AI in the Federal Administration.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

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 technological 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 barriers to market entry for technology-driven business models.

As more and more intelligent devices are connected to the internet, not only has the number of communications participants involved grown but also the number of vulnerable devices that may be misused by hackers (eg, for sending spam emails). Such devices need to be adequately protected (eg, by using individual passwords or restricted access) and respective software has to be kept updated. Between objects and devices that communicate with each other, large amounts of information and data are typically 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 their personal data either 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. Audio-Visual Media Services** regarding key data protection principles).

To protect critical information and communication infrastructure in Switzerland, the Federal Council has commissioned the Reporting and Analysis Centre for Information Assurance (*Melde-und Analysestelle Informationssicherung*, MELANI) which is part of the National Cyber Security Centre (NCSC). To prevent devices within the IoT from being misused by hackers, MELANI recommends preventive measures on its website. These measures include:

- the establishment of a separate network segment for devices connected to 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 two-factor authentication.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Broadcast Media Regulation

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 co-ordinating function for the public and policymakers. It also guarantees that basic 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 over 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.

Licensing Requirements

Broadcasters of programme services are, in principle, required to obtain a licence. Broadcasters that neither request the splitting of 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, the 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 an online video channel (such as a YouTube channel). Since the Swiss legislature strives to keep laws technology-neutral the general rules apply to the operation of online 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;
- guarantee 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 (this 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.

Investment Obligation in Swiss Film Production

On 15 May 2022, the introduction of an investment obligation in Swiss film production for streaming services was approved by the Swiss people. The amendment of the Film Act entails adjustments to the existing Film Ordinance and requires a new ordinance with implementing provisions for the implementation of the European quota and the obligation to invest in Swiss filmmaking (*Verordnung über die Quote für europäische Filme und Investitionen in das Schweizer Filmschaffen*, FQIV). The amendments include:

- an obligation for streaming service provider to invest 4% of its revenue generated in Switzerland in Swiss film productions;
- the investment may be made either directly in Swiss film production or by payment of a substitute levy which will be used to support Swiss film production; and
- an obligation for streaming service provider to broadcast at least 30% of series or films produced in Europe.

The consultation by the Federal Council will last until 17 February 2023.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

In Switzerland, the telecommunications sector is regulated at federal level. The main source of law is the TCA, which 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. 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 telecommunications service providers (TSPs), which are providers of services qualifying as telecommunications 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 OFCOM. Fixed line and mobile telephony/satellite services are regulated by the TCA and its implementing ordinances.

The latest TCA revision, which entered into force on 1 January 2021, includes improvements in the area of consumer protection (including in relation to international roaming, open internet, unfair competition and protection of children and adolescents) and provides for deregulation and administrative simplification (including abolition of the general notification and licensing requirements). Under the revised TCA, among other

things, the registration obligation for TSPs is limited to TSPs which, for the provision of telecommunications services, use:

- radio frequencies that require a licence; or
- resources administered on a national level (eg, short numbers that are assigned to emergency calls or rescue and breakdown services).

All other TSPs, while still having to comply with the obligations of the TCA, are no longer required to register with OFCOM. 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.

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, where 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 the 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).

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

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, the sector-specific regulation set out below applies to the outsourcing of business areas (infrastructure or business processes).

Swiss Banking Secrecy

Article 47 of the Swiss Federal Banking Act of 8 November 1934, as amended (the "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).

The FINMA Outsourcing Circular

Circular 2018/3 (the "Outsourcing Circular") relating to outsourcing issued on 21 September 2017 by FINMA (the supervisory authority for banks, insurers, reinsurers, stock exchanges, securities firms, collective investment schemes and audit firms) applies to banks, securities firms and insurers organised under Swiss law, including Swiss branches of foreign banks, securities firms and insurers which are subject to FINMA supervision. As of 1 January 2021, the Outsourcing Circular also applies to managers of

collective assets organised under Swiss law, including Swiss branches of foreign managers of collective assets and fund management companies with a registered office and ahead office in Switzerland as well as to self-managed *sociétés d'investissement à capital variable* (SICAVs).

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:
  (a) proper descriptions of the outsourced function;
  (b) the name of the service provider and any subcontractors;
  (c) 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 or a contract in some other format that can be evidenced in text form with the supplier setting out, among other things, 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 firms 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.

Essential Service Outsourcing

A financial market infrastructure subject to the FMIA and the implementing ordinance (FMIO), as amended (which includes a stock exchange, multilateral trading facility, central counterparty, central securities depository, trade repository or payment system), must obtain prior approval from FINMA if it wishes to outsource essential services such as risk management. If such an outsourcing is proposed by a financial market infrastructure that the Swiss National Bank (SNB) considers to be systemically important, FINMA must consult with the SNB beforehand.

When outsourcing an essential service, the financial market infrastructure must:

- carefully select, instruct and control the service provider;
- integrate the outsourced service into its internal control system; and
- monitor the services rendered by the service provider on an ongoing basis.

Reciprocal rights and duties must be set out in a written agreement with the service provider. If a financial market infrastructure outsources its services, it remains responsible for maintaining compliance with its duties under the FMIA. Outsourcing services to another jurisdiction also requires the application of appropriate technical and organisational measures to ensure the observance of professional confidentiality and data protection law. Contracting parties of financial market infrastructures whose data is to be sent to a service provider abroad must be informed. The financial market infrastructure, its internal audit function, the external audit firm, FINMA and (if systemically important) the SNB must be able to inspect and review the outsourced service.

Consolidated Rules on Outsourcing

Since 1 January 2020, consolidated rules on outsourcing also apply to both financial institutions regulated by the new Financial Institu-

tions Act (FinIA) and its implementing ordinance (FinIO), as amended and financial service providers regulated by the new Financial Services Act (FinSA) and its implementing ordinance (FinSO), as amended.

Financial institutions (which include portfolio managers, trustees, managers of collective assets, fund managers and securities firms), under the FinIA and FinIO, may only delegate tasks to third parties that have the necessary skills, knowledge, experience and authorisations to perform such tasks. The financial institution must therefore carefully instruct and supervise any such third parties. FINMA may make the delegation of investment decisions to a third party located abroad subject to an agreement on co-operation and information exchange between FINMA and the competent foreign supervisory authority (particularly if such an agreement is required under the other country's laws). If a financial institution outsources significant functions, the outsourcing service provider will be subject to information and reporting duties to, and audits by, FINMA.

The liability of financial institutions and their corporate bodies is subject to the CO. If a financial institution outsources a task to a third party, it will be liable for any damage caused by the outsourcing service provider, unless it can prove that it has diligently selected, instructed and monitored the provider (special rules may apply to fund management companies).

Financial services providers (which include client advisers and producers and providers of financial instruments), under the FinSA and FinSO, may only delegate tasks to third parties that have the necessary skills, knowledge, experience and authorisations to perform such tasks. The financial services provider must therefore carefully instruct and supervise the third parties. If a secondary (sub-contracted) financial services provider is required to provide a financial service for the principal's clients, the principal financial services provider will remain liable for:

- the completeness and accuracy of the client information;
- fulfilling the duties in relation to the information;
- the adequacy and suitability of the financial services; and
- documentation and accountability.

If the secondary financial services provider has reasonable grounds to suspect that the client information is incorrect or that such duties were not fulfilled by the principal financial services provider, it may provide its service only after it has ensured the completeness and accuracy of the information and compliance with the code of conduct.

Personal Data Protection

The outsourcing of services to an IT service provider may also impact the protection of personal data. Any data subject is protected from their 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 **3. Cloud and Edge Computing** regarding data protection principles). 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.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Trust Services, Electronic Signatures

The CO sets out the principles governing e-signatures and refers to the Electronic Signatures Act (ESA) for the technical details, which in turn refers to its respective ordinance. An electronic signature is defined as electronic data that is joined or linked logically to other electronic data and which serves to authenticate such other data.

The ESA distinguishes four levels of e-signatures:

- regular e-signatures;
- advanced e-signatures;
- regulated e-signatures; and
- authenticated e-signatures.

The authenticated e-signature in combination with an authenticated time stamp is deemed equivalent to a handwritten signature. Regulated e-signatures are not deemed equivalent to handwritten signatures; however, they may be used, for example, to evidence the authenticity of electronic invoices or to guarantee the integrity of electronically archived documents. Both authenticated and regulated e-signatures can only be obtained from a recognised provider of certification services. A list of all such providers 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 and regulated e-signatures are only available for natural persons, not for legal entities. Natural persons can, however, electronically sign on behalf of a legal entity using their personal authenticated e-signature. In addition, entities in possession of a unique business identification number may obtain a regulated electronic seal, which is essentially equivalent to a regulated e-signature.

Although e-signatures were introduced more than ten years ago, their use in Switzerland is limited. To date, only a small percentage of the population actually has an e-signature. This may be explained by Swiss law's freedom of form, enabling parties to contract without formal requirements in most cases, as well as the relatively high cost and complicated application of e-signatures and the prepayment policy applied by many online businesses, shifting the risk to the customer, who needs to trust that the other party will indeed fulfil its contractual obligations. Since payment has already been received, the online businesses generally do not have the need to verify the other customer's identity.

Electronic Identification

Following the dismissal of the Federal Act on Electronic Identification Services in the popular vote of 7 March 2021, the Federal Council

instructed the Federal Department of Justice and Police to draft a proposal for a secure governmental electronic identification (eID). From 2 September to 14 October 2021, the Federal Office of Justice conducted an informal public consultation resulting in 60 submissions. Based on the results of the consultation, the Federal Council defined the principles for the implementation of a new governmental eID and has now opened the consultation on the eID Act. The eID Act foresees, among others, that:

- the federal government shall provide an app for smartphones in which the eID can be securely managed;
- the federal government shall be responsible for issuing the eID and shall operate the infrastructure serving as a basis for the eID;
- users shall have the largest control possible over their data (self-sovereign identity) and data protection shall be ensured, among others, by the system itself ("privacy by design") and also by minimising the required data flows (principle of data minimisation) as well as by decentralised data storage;
- the Swiss eID system shall meet international standards so that it may also be recognised and used abroad in the future;
- the use of an eID shall be voluntary and free of charge; and
- all authorities, including cantons and municipalities, shall be obliged to accept the eID when they conduct an electronic identification, eg, when issuing a confirmation of residency or an extract from the debt enforcement register.

The governmental infrastructure to be created for the purpose of the eID shall also be made available for use by municipal and cantonal authorities as well as private parties.

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 the development and marketing of their services, throughout their 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 through close contacts with 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 a partner and the head of the technology and outsourcing practice and co-head of the fintech practice in the Zurich office of Lenz & Staehelin. He is also an expert on digitisation in the financial services industry. He practises in transactional and regulatory matters, outsourcing (IT and business process transactions), TMT, internet and e-commerce, data privacy, fintech, blockchain and digitisation. A member of SwissICT, SWICO, the Swiss-American Chamber of Commerce and the International Technology Law Association (ITechLaw), Lukas is a frequent speaker on topics related to fintech and digitisation.

Nadja Guberan-Flühler focuses her practice on the fields of technology, media, telecommunications and corporate law as well as outsourcing transactions, licensing, e-commerce and data protection matters. She works as an associate in the Zurich office of Lenz & Staehelin and is a member of the firm's technology and outsourcing, corporate and M&A, intellectual property and real estate practice groups.

Lenz & Staehelin

Brandschenkestrasse 24
CH-8027
Zurich
Switzerland

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

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com