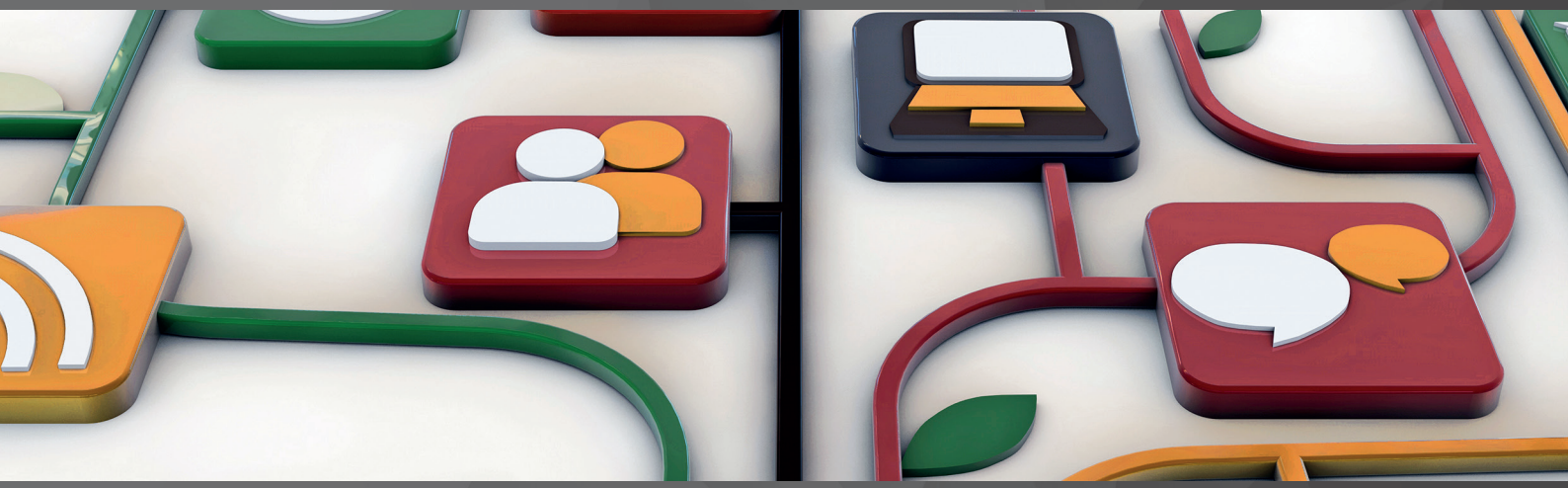
International
Comparative
Legal Guides



Technology Sourcing 2021

A practical cross-border insight into technology sourcing

First Edition

Featuring contributions from:

Arioli Law

ASBZ Advogados

Astrea

Bird & Bird

Bryan Cave Leighton Paisner LLP

BSN Bufete Sánchez Navarro, S.C.

Cliffe Dekker Hofmeyr Inc.

Dana Associés

Fieldfisher

Goodmans LLP

Gorriceta Africa Cauton & Saavedra

Ikeyi Shittu & Co.

SHUSAKU·YAMAMOTO

TMT Law Practice

Wistrand Law Firm

ICLG.com

Expert Analysis Chapter

Q&A Chapters

Switzerland

Arioli Law

Martina Arioli

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

No, Swiss law does not specifically regulate the procurement of technology products and services in the private sector. Of course, mandatory statutory provisions must be adhered to that govern certain aspects of technology sourcing transactions, such as employment law, data protection law and merger law.

A number of industries are subject to strict secrecy obligations:

Banking institutions are subject not only to Swiss banking secrecy (Article 47 Federal Banking Act) but also to multiple regulatory requirements including circulars issued by the supervisory authority (the Swiss Financial Market Supervisory Authority (FINMA)) when procuring technology solutions. Similarly, insurance companies are subject to statutory regulations and, in particular for outsourcing of significant functions or partial outsourcing of control functions to third parties, to the FINMA Outsourcing Circular.

In the telecoms sector, providers are subject to telecoms regulations (Federal Telecommunications Act) which contain secrecy obligations.

The healthcare sector is subject to extended secrecy obligations that render additional safeguards in technology sourcing contracts necessary.

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

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

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

On a federal level, the public procurement process is governed by the revised Federal Act on Public Procurement (PPA) of 21 June 2019. The cantons unanimously adopted the revised Intercantonal Agreement on Public Procurement (*Interkantonale Vereinbarung über das öffentliche Beschaffungswesen*; *IVöB*) on 15 November 2019. Both revisions aim at harmonising the procurements principles on federal and cantonal level, eliminating ambiguities and adapting court practice. In particular, a paradigm shift has been implemented from favouring the most economic tender to the best tender in terms of quality.

The basic features of the regulatory regime are transparency, objectivity and impartiality, the prevention of conflicts of interest, corruption and negative impacts on competition. Further, all tenderers are to be treated equally at all stages of the procedure and safeguarding at all times the confidentiality of the process. In addition, tenderers must comply with minimum requirements regarding health and safety of their workforce, equal pay, compliance with employments laws and protection of the environment.

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No, there are no mandatory minimum or maximum terms for a contract for the supply of technology-related solutions and services; the parties are free to determine the duration.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No, there are no mandatory notice periods for technology sourcing contracts. However, when negotiating a notice period, the customer should take into account the time it takes to move to an alternate provider in order to ensure a smooth transition and migration.

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes, the Swiss Civil Code contains in Article 2 the general principle that all must act in good faith in the exercise of their rights and in the performance of their obligations. The manifest abuse of a right is not protected by law. This overarching principle of good faith is not only enshrined in law but is of utmost importance in Swiss daily business.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Technology-related solutions and services agreements may contain elements of the statutory provisions relating to contracts for work and services, to sales contracts, and to corporations. Consequently, the applicable statutory provisions and corresponding remedies are highly dependent on what contractual obligations of the outsourcing agreement have been breached. Given that the statutory provisions are not mandatory, the parties are free to determine remedies in the outsourcing agreement, such as:

- remediation of defects within determined time limits, including, e.g., the replacement of hardware;
- monetary compensation for damages, including liquidated damages/penalties;
- reduction of fees;
- step-in rights; and
- termination or rescission of the agreement.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Additional protection measures may include:

- specific warranties;
- regular charge or a service provision review mechanism;
- contract change management; and
- audit and benchmarking.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Given that Swiss law does not provide for specific termination provisions applicable to technology sourcing agreements, the parties typically agree on termination for cause and termination for convenience, including the respective notice periods. In particular, as regards termination for material breach, it is recommended that scenarios that constitute such material breach are specifically agreed on and respective contractual obligations are spelt out. If a party adheres to the contractually stipulated termination provisions, claims for damages from the terminated party should not arise. However, this does not necessarily preclude dire discussions on whether a breach may be deemed material or not.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties are free to exclude or agree upon additional termination rights such as insolvency events, change of control and multiple/persistent minor breaches.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

Pursuant to Swiss law, the parties cannot exclude or limit liability for damages caused by intent or gross negligence. Further, it is not possible to exclude or limit liability for death or personal injury resulting from a negligent breach of contract.

Typically, the provider aims to extensively exclude liability for indirect and consequential loss or damages, for loss of business, profit or revenue. By contrast, the customer typically aims to have such damages contractually deemed as direct damages.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes, the parties may agree on a financial limit on liability and indemnities, subject to the limitations set out in question 2.8. The cap can be a fixed amount or a percentage of the contract value.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No, these principles apply to all of the aforementioned types of technology procurement contracts.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

There are no main methods for dispute resolution used in Switzerland and there are no statutory rules on contract management, governance and escalation in Swiss contract law. Thus, it is recommended that detailed provisions are included in the agreement governing a dispute resolution process before a party can resort to a court or arbitration. Any dispute resolution process must, however, be limited to a resolution time period to ensure expedited resolution. Typically, the parties agree upon an internal escalation procedure along the lines of the respective company's hierarchy and, ideally, set timeframes in order to reach a settlement in due time. If the parties fail to reach a settlement despite escalation or in the absence of such contractual escalation, the parties can agree to involve a mediator; however, mediation is still rare in Switzerland for business-related disputes.

If a party initiates civil proceedings, the first hearing before the judge/court aims at reconciliation. Only in the event such reconciliation fails does the court proceed to address the legal claim(s) put forward.

Further, the agreement may include provisions on arbitration.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

Typically, the parties agree on the rights to use pre-existing IP and the allocation of rights in materials developed in the context of the technology sourcing agreement ("work products"). Further, depending on the transaction, the transfer of ownership in intellectual property rights or the assignment of licences may be agreed upon. It is advisable to specifically detail any and all intellectual property rights in the technology sourcing agreement in order to avoid difficult termination negotiations.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

For the transfer, lease or license of intellectual property rights, the written form is recommended. Further, it is strongly recommended to register transfers of trademarks and patents in the respective registries administered by the Swiss Federal Institute of Intellectual Property as soon as possible.

Third-party intellectual property must be taken into account as the relevant licence agreements may require the consent of such third party.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

The Federal Act Against Unfair Competition and the Criminal Code provide for penalties for the breach of trade secrets and the exploitation of such secrets.

It is recommended to protect know-how, trade secrets and other business critical confidential information by including extensive confidentiality clauses in the outsourcing agreement that provides for penalties to be paid in the event of breach. Note that EU Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure does not apply in Switzerland.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

Given that Switzerland is not a member of the EU, the General Data Protection Regulation (GDPR) – as a rule – does not apply in Switzerland. However, the GDPR may apply to Swiss companies for the processing of personal data under Article 3 GDPR, as well as in multijurisdictional outsourcings. Where the GDPR applies to the controller and the outsourced service involves processing of personal data, a data processing agreement in compliance with Article 28 GDPR must be included in the outsourcing agreement. Such data processing agreement shall also include the technical and organisational data security measures implemented by the supplier.

The revised Federal Data Protection Act (FDPA) will enter into force in 2022, containing provisions similar to the GDPR pertaining to data processing, as well as the transfer of data to countries without an adequate level of data protection.

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

Under the current FDPA, the following requirements for outsourcing transactions apply:

- the parties should conclude a written processing agreement, in particular, as this will be mandatory under the revised FDPA;
- personal data may only be processed by the supplier in accordance with the purpose defined and within the limits of the processing permitted to the customer itself and pursuant to the instructions of the customer;
- the processing of personal data must not be prohibited by a statutory or contractual duty of confidentiality; and
- the customer shall ensure that the supplier provides for data security in accordance with the requirements of the Ordinance to the FDPA (currently under revision) by implementing adequate technical and organisational measures, taking into account the purpose, as well as the nature and extent of the processing, an assessment of the possible risks to the data subjects and the current state of the art. The technical and organisational measures shall ensure confidentiality, availability and integrity of data by protecting data from unauthorised or accidental destruction, accidental loss, technical faults, forgery, theft or unlawful use, unauthorised alteration, copying, access or other unauthorised processing.

For cases of cross-border outsourcing, the Federal Data Protection and Information Commissioner (FDPIC) provides a sample Swiss Transborder Data Flow Agreement, which allows data processors to comply with the requirements stipulated in the FDPA regarding cross-border data transfers.

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.

In May 2020, FINMA published a supervisory notice on the obligation to report cyber attacks for banks, insurance companies and other institutions under its supervision. FINMA stipulates that relevant cyber attacks must be reported within 72 hours of the incident being discovered. The revised FDPA will introduce such a reporting obligation applicable to all data controllers. For FINMA-supervised institutions, this entails that both the supervisory reporting obligation and the data protection reporting obligation will need to be adhered to.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

Yes, personal data can be transferred outside of Switzerland. However, the parties must either: obtain the consent of each data subject individually; or put measures in place to ensure that the data is adequately protected in the relevant jurisdiction, such as sufficient contractual guarantees, or binding corporate rules (BCR), provided the processing takes place within a legal entity or among legal entities under common control and all involved parties are subject to the BCR. Under the revised FDPA, the parties no longer need to notify the FDPIC if the cross-border transfer is based upon pre-approved standard contractual clauses or BCR.

The *Schrems II* decision by the European Court of Justice of July 2020 does not apply in Switzerland; however, it of course

has a great impact on the validity of cross-border transfers based upon standard contractual clauses given that Switzerland follows the EU regime. In order to ensure compliance with the most current requirements, it is worth double checking the website of the FDPIC prior to any transfer taking place.

5.3 Are there any legal and/or regulatory requirements concerning information security?

The Swiss government issued the National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018–2022, which contains measures to safeguard Switzerland's independence and security and to protect it from cyber threats. The strategy paper offers a few specific instructions for action as, ultimately, the individual players are and remain responsible for their own protection. Further, no specific statutes have been enacted so far that go beyond the general obligations pursuant to the Swiss FDPA to implement appropriate technical and organisational measures to ensure data security when processing personal data. The draft Information Security Act that shall apply to the Swiss Federal government has yet to enter into force. For the private sector, information security is left to the responsibility of self-regulatory regimes and certifications such as ISO. Guidelines and checklists have been issued by various organisations, such as the "Information Security Checklist for SMEs" by the Reporting and Analysis Centre for Information Assurance MELANI (May 2018) or the Cloud Guidelines of the Swiss Bankers Association, a guide to secure cloud banking (March 2019). To boost activities in the area of cyber-risk awareness, on 30 January 2019 the Federal Council decided to set up a competence centre for cybersecurity, the National Cyber Security Centre, as a first point of contact for questions on cybersecurity.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Article 333 of the Swiss Code of Obligations (CO) stipulates that if the employer assigns its business or a business unit to an acquirer, the employment relationship of any employee affected automatically transfers to the acquirer, unless the affected employee objects to such transfer. This also applies to mergers, splits or asset transfers in accordance with Article 27 of the Swiss Merger Act.

The previous employer is obliged to inform or consult with the employees' representatives or, if there is no representation, with the employees themselves in good time before the transfer takes place (Article 333a CO).

The employment agreements are automatically transferred to the acquirer on essentially all existing terms and conditions, including benefits granted under the employment agreement or based on a collective bargaining agreement, as well as accrued holiday entitlements. After the transfer, the acquirer can modify the employment terms – see question 7.5.

The former employer and the acquirer are jointly and severally liable for an employee's claims that (i) are due prior to the transfer, or (ii) will become due up to the date the employment relationship can effectively be terminated or until its actual termination based on the employee's objection to the transfer.

6.2 What employee information should the parties provide to each other?

There is no statutory rule on what information must be exchanged by the parties to an outsourcing agreement. Prior to the transfer date, the data on employees disclosed to the acquirer must be limited to a "need to know" basis and should be anonymised to the extent possible. Information may include details on employment terms and conditions, function, seniority level, salary and notice period.

Upon transfer, the acquirer must be provided with all necessary information for the performance of the employment agreements in order for the acquirer to fulfil its obligations as the employer.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

As a rule, such termination would contravene Article 333 CO. However, if the respective notice period is observed, the employment agreement may be terminated after or even prior to the transfer.

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

Yes, after the transfer, the new employer may modify the employment terms of the transferring employee subject to the employee's consent and provided that the modification pertains to non-material aspects only.

The acquirer may also terminate the employment agreements and offer new agreements on changed terms of employment (constructive dismissal). The new terms can enter into force only once the contractual notice periods have expired.

6.5 Are there any pensions considerations?

When employees are transferred under Article 333 CO, the employees' vested benefits under the former employer's pension scheme are transferred to the acquirer's pension scheme. After the transfer, the employees' pension benefits are calculated according to the new scheme's regulations.

If the workforce that forms part of the former employer's pension scheme reduces substantially, the respective pension scheme must be partially liquidated. The employees then have individual or collective claims to a portion of the non-committed funds (free reserves) in addition to their ordinary claims to the vested benefit.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

If the outsourcing agreement entails the transfer of business offshore, the parties need to assess whether the employment contracts of the affected employees actually transfer by operation of law given that Article 333 CO only applies if the business concerned preserves its identity post-transfer.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

The revised Outsourcing Circular 2018/03 of the Swiss Financial Market Supervisory Authority FINMA, applicable as of 1 April 2018, contains regulatory requirements for outsourcing by banks, securities dealers as well as (new) insurance companies organised under Swiss law, including Swiss branches of foreign banks, securities dealers and insurers that are subject to FINMA supervision. The Outsourcing Circular 2018/03 sets out provisions on the selection, instruction and control of suppliers, including a comprehensive audit right, as well as provisions to secure availability of data. The provisions on data protection contained in the previous version of the FINMA Outsourcing Circular have been dropped to avoid inconsistencies with general data protection laws.

Article 47 of the Swiss Federal Banking Act protects customer-related data from disclosure to third parties and applies to all banking institutions in Switzerland (banking secrecy). An outsourcing agreement with a customer subject to banking secrecy must therefore contain the supplier's obligation to comply with the banking secrecy rules. Further, any disclosure of non-encrypted data to a supplier is only permitted with the express consent of each banking customer; such consent may be obtained based upon the bank's general terms of business applicable to the individual customer contract.

Specific notification requirements must be considered in connection with outsourcings by other players in the Swiss financial market.

In particular, insurance companies must notify FINMA of any outsourcing of essential functions deemed a change of business plan. The notification procedure can ultimately be deemed an approval process given that FINMA may open investigations within four weeks after notification has been submitted.

Financial market infrastructures such as stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories or payment systems are subject to the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (FMIA) and must obtain prior approval from FINMA if it wishes to outsource essential services such as risk management.

Furthermore, asset managers, trustees, managers of collective assets, fund management companies and securities firms must comply with the Financial Institutions Act (FinIA) and, similarly, client advisers and providers of financial instruments must comply with the Financial Services Act (FinSA) when outsourcing tasks to third parties.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

Generally, the outsourcing relationship is based on a master services agreement between two independent companies. For global outsourcing transactions involving multiple group entities, the contractual structure is more complex: in a centralised contractual set-up, the customer procures the provider's services on behalf of its group affiliates, whereas in a decentralised contractual set up, the customer affiliates procure services from the provider directly as contractual parties.

Further, the customer and provider may choose to set-up a joint venture or enter into a contractual joint venture or partnership agreement. The customer may also establish an (offshore) captive entity.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

The definition of service levels and service credits depends entirely on the technology outsourcing transaction.

In the Statement of Work, the parties define the services to be provided and the service levels, as well as the service criteria by which performance can be measured (key performance indicators). This entails detailed reporting and monitoring. In the event that the provider does not achieve the agreed-upon service levels, a (relatively small) amount is deducted from the service fees payable to the provider as a service credit. Service credits for a specific time period are usually capped at an at-risk amount in the range of 5% and 15% of the fees due in that particular time period.

The service credits shall incentivise the provider to consistently achieve the agreed service levels and to facilitate a partial compensation of the customer for poor service without the need to pursue a claim for damages or terminate the agreement.

Service credits are typically the sole remedy of the customer for the particular failure concerned, however, without prejudice to the customer's more extensive rights in relation to more serious contract breaches or persistent performance failures, *cf.* questions 2.4 and 2.7.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

The most common charging methods include cost plus (actual costs incurred by the provider plus a pre-agreed profit margin), fixed pricing for regular and predictable volume and scope of services, or consumption/transaction-based charging.

The outsourcing agreement should provide for a mechanism for cost control and adequate adjustment of charges, including:

- charge variation mechanisms;
- change management procedures;
- service level credits or bonus/malus;
- measures to share cost savings between the parties and provide an incentive to the provider to achieve these;
- auditing;
- benchmarking;
- disputed charges; and
- a pre-agreed inflation adjuster.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

For the transfer of third-party contracts, the customer shall first assess whether such transfer is permitted under the third-party contract. If the transfer is contractually excluded, the parties shall assess whether the contract can be at least managed by the provider or whether the contract should be terminated. If the transfer requires the consent of the third party, such consent shall be obtained in writing. If the transfer is not excluded or not made subject to consent, it suffices to inform such third parties of the transfer to the provider in writing to effect the transfer.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

The transfer of assets within an outsourcing agreement may trigger corporate income taxes, real estate transfer tax, federal securities transfer tax, and VAT. Pursuant to Swiss law, every transfer of assets to the provider constitutes a supply of goods or services and is, in principle, subject to VAT. If transferred assets are part of a transferred business entity, VAT must be notified. Intragroup outsourcing may result in a VAT leakage, which can be neutralised by group taxation.

Intragroup outsourcing must be at arm's length and in line with general transfer pricing principles.

For multijurisdictional outsourcings, it is recommended to consider holistic tax planning in order to avoid double taxation, to reduce source income taxes and, for intragroup outsourcings, identify tax optimising measures.

The termination of contracts without adequate compensation and/or a notice period may give rise to taxation of a constructive dividend/profit shift. According to prevailing doctrine, the mere shift of functions should not be taxed.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

For licensing on-premise, the customer requires a sophisticated IT department and/or secures the support from the licensor or its agents for purposes of smooth roll-out of software updates. Otherwise, the same principles apply as to cloud computing.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

The customer should ensure the implementation of stringent security measures for the provider's access to its infrastructure, limit the access granted to the provider's personnel, conclude a confidentiality agreement with the provider and the individual support staff members, and limit the access to personal data as far as possible.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

Escrow agreements are used in Switzerland and they are enforceable; however, it would be exaggerating to call this common practice. Many customers choose not to conclude an escrow agreement despite the risks of a lock-in to their provider as they deem it unfeasible to make use of the source code themselves or by third parties once released from escrow.

9 Cloud Computing Services

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services?

No, there are no Swiss statutes or regulations that specifically regulate the procurement of cloud computing services.

On 11 December 2020, the Federal Council adopted a cloud strategy for the Federal Administration in order to use cloud services to support its digital transformation, to ensure having more IT sourcing options, increasing agility and speed, developing scalable and resilient platforms, and reducing costs. However, in particular during the COVID-19 pandemic, it became clear that the Swiss government is still very much at the outset of the digital transformation.

The Federal Council as well as the private sector are closely monitoring the developments abroad, in particular the GAIA-X initiative, and assessing possible involvement, including a potential GAIA-X hub in Switzerland. Swiss companies are already involved in GAIA-X today, and there have been no barriers to access for Swiss enterprises to date.

9.2 How widely are cloud computing solutions being adopted in your jurisdiction?

For years, the use of cloud computing solutions has been the subject of heated debate in Switzerland, which has displayed a certain reservation towards cloud computing solutions. This stems not only from issues arising based upon data protection and data security, but moreover from concerns in view of trade secrets and professional secrecy obligations, in particular in the financial sector, health sector and further sensitive sectors, as well as law firms. To address these concerns, large and small players are now offering cloud solutions with guaranteed storage in Switzerland.

In spite of the heated debate, in reality, cloud computing solutions are widely used in Switzerland, not only by private citizens but also private companies.

9.3 What are the key legal issues to consider when procuring cloud computing services?

The key issues to consider are, in particular:

- assurances of the provider as regards business continuity and disaster recovery;
- information security and data security;
- data portability/contractual migration obligations in order to avoid lock-in in the event of termination/expiry of the contract, including also the support of the cloud provider and its assurance to work with a new supplier, if necessary; and
- guarantees by the cloud provider regarding professional secrecy.

10 AI and Machine Learning

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI-based solutions or technologies?

No. Irrespective of the fact that Switzerland deems itself to be a hub in the development of AI solutions by research institutions and private companies and private/public partnerships, Switzerland has to date not adopted any specific laws and regulations on AI. Interestingly, FINMA noted already in its Circular 2013/8 that "supervised institutions must document the key features of their algorithmic trading strategies in a way that third parties can understand".

The Federal Council deems AI an essential component of advancing digitalisation with considerable potential for innovation and growth. Accordingly, in 2020 the State Secretariat for

Education, Research and Innovation (SERI) issued Guidelines on the responsible use of AI within the public sector.

Given that Switzerland is not a member of the EU/EEA, the Proposal for a Regulation laying down harmonised rules on artificial intelligence (draft EU Artificial Intelligence Act), issued on 21 April 2021, will not take effect in Switzerland. Nevertheless, the EU Artificial Intelligence Act, once enacted, will have an impact on Swiss businesses active in the field, similarly to the GDPR or the EU Medical Device Regulation (MDR). Potentially, Switzerland will adopt its own legal framework on the procurement and use of AI at some point in time.

10.2 How is the data used to train machine learning-based systems dealt with legally? Is it possible to legally own such data? Can it be licensed contractually?

There are no statutes or regulations that govern the training data of AI in Switzerland. Ownership of data has occasionally been the topic of academic debate in recent years; however, neither scholars nor the legislator have embraced the notion of data ownership. For the lack of a better term, however, technology sourcing contracts often deploy the term "data ownership" in order to allocate responsibility and a so-called "economic power of disposal" ("*wirtschaftliche Verfügungsmacht*"), be it to the provider or the customer. In order to address the access and use of data beyond data protection compliance, technology sourcing contracts contain provisions that can be deemed license-like granting of rights and obligations.

10.3 Who owns the intellectual property rights to algorithms that are improved or developed by machine learning techniques without the involvement of a human programmer?

Pursuant to Swiss law, software is typically protected by copyright law; in very exceptional cases patent protection can be obtained. However, under the Swiss Copyright Act, as well as under the Swiss Patent Act, only a human creation/invention can obtain legal protection. Accordingly, there must be a "human in the loop", be it the owner, the original developer or the user of the AI.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there are no Swiss laws or regulations that specifically regulate the procurement of blockchain-based solutions.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

Blockchain has been adopted in particular in the context of disruptive fintech solutions, and for some time, Switzerland has become a hub for blockchain start-ups. This has led Switzerland to enact the new DLT Act (Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology) entering into force on 1 August 2021. This DLT Act contains various improvements to the Swiss legal framework in connection with the use of decentralised technologies and blockchain, including in particular the introduction of ledger-based securities that enable the digitisation of shares and other rights.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

Blockchain technology is decentralised, immutable, and transparent. Consequently, blockchain applications may pose a challenge as regards compliance with data protection law. The decentralisation means that there is no one responsible for compliance, i.e. there is no controller in the sense of data protection laws. This applies in particular to public (permissionless) blockchain. Further, the immutability of data on the blockchain may be in conflict with the data protection principle of data accuracy.

In order to ensure compliance, companies tend to deploy private (permission-only) blockchains for internal applications only in order to be able to select the participants, manage the transaction content, and delete data in the event it is rendered inaccurate. Alternatively, applications are deployed with which transaction-related personal data is stored outside the blockchain application itself (off-chain). Only the cryptographic hash values including the timestamp remain on the blockchain itself. Further, the transaction-related personal data can be encrypted on the blockchain itself and the private key is only available to a limited group of authorised individuals.

Martina Arioli has been listed by *Chambers Europe* for TMT since 2019 and recognised as one of Switzerland's leading business lawyers since 2016 by *Who's Who Legal*. Martina Arioli has been selected as Thought Leader Data in Switzerland since 2019 and won the Client Choice Award Data Switzerland 2020.

Martina Arioli is an experienced legal counsel, with almost 20 years of international practice, specialised in IT law and outsourcing. She has supported outsourcing engagements in all stages, from contract drafting, negotiating global and local agreements to implementation and transition, conflict mediation, termination and resourcing to new suppliers. Martina Arioli combines in-depth knowledge on complex contractual matters in outsourcing and information technology projects with the experience of implementing such global projects as an in-house lawyer. Previous positions include senior roles at Zurich Insurance Company and UBS AG, as well as the law firm Walder Wyss Ltd.

Martina Arioli studied law, philosophy and political science at the University of Bern from which she graduated in 1996 (*magna cum laude*), passed the Bar in 1999 with excellence and received an LL.M. from London School of Economics and Political Science (LSE) in IP in 2001. Since 2008, she has chaired a prestigious annual conference on data protection in Switzerland. She lectures law at various Swiss universities.

Arioli Law
Napfgasse 4, 8001 Zurich
Switzerland

Tel: +41 44 201 66 11
Email: martina.arioli@arioli-law.ch
URL: www.arioli-law.ch

Arioli Law is a boutique law firm established in 2013 in the heart of Zurich. It is one of the first one-woman law firms to specialise in outsourcing, IT law, data protection law and entertainment law.

The renowned Swiss business magazine *BILANZ* has consistently ranked Arioli Law amongst the Switzerland's 10 top law firms in TMT and IP law since the first ranking issued in 2017. Arioli Law is listed as "highly recommended" in the ranking of Leaders League for Technologies, Internet & Telecommunications – IT & Outsourcing 2021.

www.arioli-law.ch

MARTINA ARIOLI
LAW FIRM

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group