

International Comparative Legal Guides

Technology Sourcing 2026

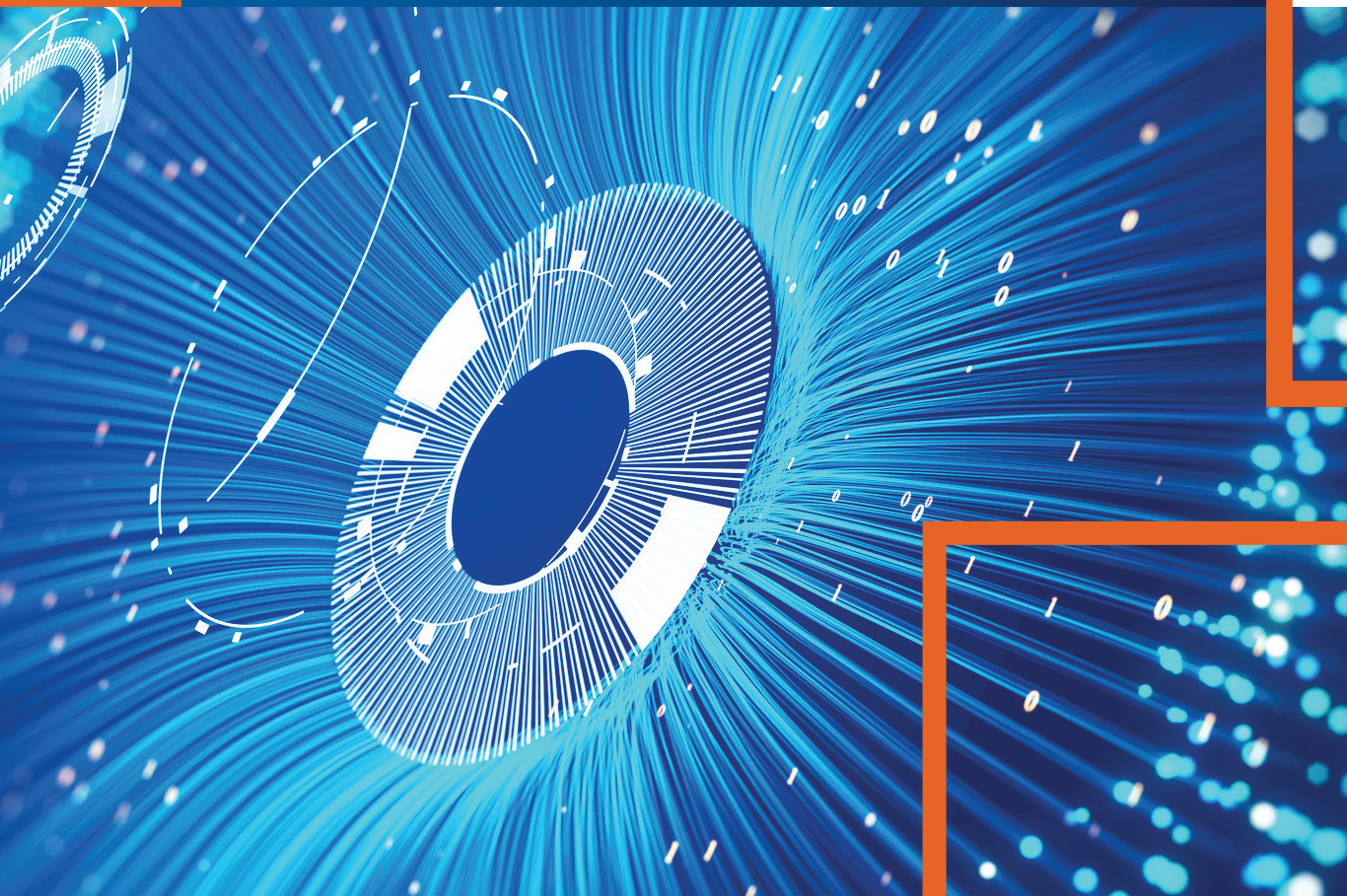
A practical cross-border resource to inform legal minds

Sixth Edition

Contributing Editors:

Will Bryson & Ben Woodfield

Bird & Bird LLP



iclg

Expert Analysis Chapters

1

Sourcing AI Solutions

Will Bryson & Ben Woodfield, Bird & Bird LLP

10

The Future of Strategic Sourcing: AI, Agility and the New Commercial Model

Kerry Hallard, Global Sourcing Association

Q&A Chapters

14

Armenia

Narine Beglaryan, Artur Hovhannisyan,
Shushan Stepanyan & Yevgenya Nikoghosyan,
Concern Dialog Law Firm

22

Australia

Kate Morton & Gianluca Pecora, Bird & Bird

32

Austria

Wolfgang Freund, Grama Schwaighofer Vondrak
Rechtsanwälte GmbH

40

Cyprus

Zena Spanou & Angelica Achilleos,
Markos P. Spanos & Co LLC

49

France

Stéphane Leriche, Bird & Bird

60

Germany

Dr Henriette Picot, Michaela von Voß,
Dr Rolf Schmich & Vincent Kirsch, Bird & Bird LLP

71

Hong Kong

Wilfred Ng, Hwee Yong Neo, Jennifer Lau &
Rachel Tang, Bird & Bird

85

India

Harsh Kumar, Indraneel Chakraborty &
Vanshika Tandon, Kaizen Law

96

Japan

Aya Saito & Fumiko Masuda, Bird & Bird

104

Malaysia

Lo Khai Yi, Ong Johnson & Aida Suhailah
Halim Hong & Quek

112

Nigeria

Josephine Tite-Onnoghen, Ishaq Apalando &
Emmanuel Matuluko, Ikeyi Shittu & Co.

121

Philippines

Kerwin K. Tan, Veronica S. Balbin,
Jose Maria B. Buenagua, Tan Hassani and Counsels

130

Saudi Arabia

Peter Koh, Charlie Christie, Nikita Manro &
Reem Abu Alsaud, Bird & Bird

142

Singapore

Jeremy Tan & Chester Lim, Bird & Bird ATMD LLP

150

South Africa

Tayyibah Suliman, Izabella Gutlar-Balkovic, Sadia Rizvi
& Taryn York, Cliffe Dekker Hofmeyr Incorporated

160

Switzerland

Martina Arioli, Arioli Law

169

Taiwan

Bo-Sen Von, Tsung-Yuan Shen, Rachel Chen &
Effie Peng, Lee and Li, Attorneys-at-Law

178

United Kingdom

Will Bryson & Ben Woodfield, Bird & Bird LLP

194

USA

Sonia Baldia, Kilpatrick Townsend & Stockton LLP

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, there is no specific regulation governing private sector procurement of technology products and services under Swiss law. However, technology sourcing is often shaped by mandatory or semi-mandatory rules outside procurement law, in particular data protection, employment law, competition/merger control, professional secrecy, financial market regulation, product safety and sector-specific supervisory requirements.

Certain industries are subject to stricter regulatory frameworks:

- Banking and insurance: Institutions must comply with banking secrecy (Art. 47 Federal Banking Act) and sector-specific Swiss Financial Market Supervisory Authority (FINMA) requirements when procuring technology.
- Telecommunications: Providers are subject to the Federal Telecommunications Act, which includes secrecy obligations.
- Healthcare: Private providers must comply with rules on medical devices, professional secrecy, cybersecurity, and data protection. Software used in diagnosis or treatment may qualify as a medical device subject to Swissmedic and Medical Device Regulation (MDR)-based requirements.
- Professional secrecy: Art. 321 Swiss Criminal Code imposes secrecy obligations on professionals (e.g. medical, legal). IT providers may qualify as auxiliary persons and must be contractually integrated into the confidentiality framework.

It is essential to align sourcing contracts with the applicable sector-specific obligations. This is particularly important for regulated customers, critical or outsourced functions, access to confidential information and the processing of personal data.

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?

Yes, procurement by government and public sector bodies in Switzerland is regulated. Federal and cantonal public procurement laws apply, depending on the authority and project scope.

A competitive tender procedure (open, selective, or invitation) is generally required above certain thresholds; direct awards are permitted only in exceptional cases.

At the federal level, procurement is governed by the revised Federal Act on Public Procurement of 21 June 2019. The cantons adopted the harmonised Inter-Cantonal Agreement on Public Procurement (IVöB 2019) to align core principles. A key reform in 2019 was the shift from awarding to the lowest-priced offer to selecting the most advantageous tender based on quality.

Core features of the regime include:

- Transparency, equal treatment, non-discrimination, competition, economic use of public funds, and confidentiality throughout the process.
- Prevention of conflicts of interest, corruption, and market distortion.
- Mandatory compliance with labour, health and safety, equal pay, environmental, and (since 1 January 2024) cybersecurity standards under the new Information Security Act.

Public procurement law also applies to private entities when they perform public tasks on behalf of government bodies.

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?

There is no technology-specific statutory notice period. 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. Depending on the contractual qualification, statutory termination rules may nevertheless be relevant; for example, mandate-like service arrangements may be terminated at any time, subject to liability if termination occurs at an inopportune time.

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, Art. 2 Swiss Civil Code enshrines the fundamental principle of good faith, requiring that rights be exercised and obligations fulfilled in a fair and honest manner. The manifest abuse of a right is not protected by law. This overarching principle is not only codified, but also deeply rooted in Swiss legal practice and everyday business conduct.

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

Technology sourcing agreements often combine elements of work, sales, and service contracts. Remedies under Swiss law depend on the nature of the breached obligation and the contract's qualification. As most provisions are non-mandatory, the parties typically define specific remedies, such as:

- remediation within set deadlines (e.g. bug fixes, hardware replacement);
- monetary compensation, including liquidated damages or penalties;
- fee reduction (e.g. service credits);
- step-in rights; or
- termination or rescission.

Absent contractual provisions, statutory remedies under the Swiss Code of Obligations apply, depending on the contract type and severity of the breach.

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?

Typical customer protection measures may include:

- specific warranties and representations;
- service levels, service credits, service reviews and benchmarking;
- acceptance procedures, defect remediation, change control and governance; and
- audit rights, security controls, subcontractor approval, data return/deletion, exit assistance, business continuity, disaster recovery, escrow where appropriate and Intellectual Property (IP)/data indemnities.

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

Swiss law does not provide specific termination rules for technology sourcing agreements, so parties typically agree on termination for cause and for convenience, including notice periods. To minimise the risk of damage claims, the agreement should clearly define what constitutes a material breach and specify the related obligations. Even where the contractual process is followed, disputes may arise over whether the relevant breach, dependency failure or regulatory event justified termination.

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. Other common triggers include loss of regulatory approval, material security incidents, breach of confidentiality or data protection obligations, repeated Service Level Agreement failures, unlawful subcontracting, sanctions exposure and failure to maintain required insurance or certifications.

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

Pursuant to Swiss law, liability for intent or gross negligence, as well as for death or personal injury due to negligence, cannot be excluded or limited in advance.

Contractual exclusions of liability for indirect or consequential damages such as loss of profit, revenue, or business are common. While providers seek broad exclusions, customers often negotiate to classify such losses as direct damages to preserve compensation claims.

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, the general legal principles discussed above apply to all of the listed types of technology procurement contracts. However, their concrete application may differ depending on the contractual structure and regulatory context.

- (a) Software licensing is usually structured as a licence or mixed/*sui generis* agreement. Depending on the arrangement, elements of sales, lease, work contract or service law may be relevant.
- (b) Cloud computing contracts raise additional issues regarding data protection, cross-border data transfers, subcontracting, access by foreign authorities, information security, resilience, auditability, portability, exit, data return/deletion and service continuity, often governed by elements of both service and mandate law.
- (c) Outsourcing contracts may trigger regulatory, public procurement, data protection, secrecy, audit, business continuity and concentration-risk requirements, particularly in the financial sector and for public sector customers.
- (d) AI-based or machine learning solutions are not yet subject to a dedicated AI legislation in Switzerland. Nevertheless, such contracts should address use-case classification, model and data governance, training/fine-tuning data, output quality, explainability, human oversight, bias, IP rights, regulatory change, auditability and liability.
- (e) Blockchain-based solutions fall under Switzerland's generally technology-neutral and innovation-friendly

legal framework. Depending on the use case, financial market, distributed ledger technology (DLT), anti-money laundering, securities, data protection, insolvency, tax, cybersecurity and private international law issues may arise; immutability also requires careful treatment of correction, deletion and governance obligations.

In all cases, it is essential to tailor the contractual framework to the specific risks and legal considerations of the technology involved.

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?

Swiss law does not mandate specific dispute resolution methods or escalation procedures for technology contracts. Accordingly, parties typically define their own process, which often includes:

- Internal escalation clauses, with defined timeframes and hierarchy levels.
- Mediation or other alternative dispute resolution mechanisms to resolve disputes amicably.
- Civil court proceedings, which usually begin with a mandatory conciliation hearing.
- Arbitration, especially for complex or cross-border contracts, offering flexibility and international enforceability.

It is recommended to include clear, time-bound dispute resolution clauses, tailored to the complexity and value of the contract.

4 Intellectual Property Rights

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

In technology sourcing agreements, IP rights are typically addressed through clear contractual allocation:

- Pre-existing IP, supplier tools, standard software, libraries, templates, methodologies and know-how normally remain with the original right holder, with the other party receiving the licences necessary to perform or receive the services.
- Newly developed work products should be allocated expressly. Depending on the transaction, custom software, interfaces, documentation, configurations, reports, models or other deliverables may be assigned to the customer, licensed to the customer, or retained by the supplier with customer-specific use rights.

The agreement should clearly specify ownership, scope of use rights, sublicensing, and territorial and temporal limitations. It should also address adaptations, derivative works, data and training data, open-source components, third-party rights, escrow or exit rights, and the customer's right to maintain, modify and further develop the solution after termination. Depending on the transaction, parties may also agree on the transfer of ownership, exclusive or non-exclusive licences, or the handling of open-source components. Precise IP provisions are essential to avoid disputes, especially in the context of termination, exit support, or further development.

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

Under Swiss copyright law, economic copyrights are assignable and no statutory form is required for their assignment; an assignment may therefore be agreed in writing, orally or, in limited circumstances, impliedly. However, a written agreement is strongly recommended, in particular for evidentiary purposes. By contrast, assignments of trademarks, patents and designs are subject to written form requirements. It is also advisable to promptly register any transfer with the Swiss Federal Institute of Intellectual Property to ensure its effectiveness against third parties.

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

Yes. Under Swiss law, trade secrets and business-critical know-how are protected by:

- the Federal Act Against Unfair Competition (UCA), which prohibits unlawful acquisition, use, and disclosure of trade secrets (Art. 4 lit. d and Art. 5 UCA); and
- the Swiss Criminal Code, which penalises the unlawful exploitation or disclosure of trade or business secrets (Art. 162 Swiss Criminal Code).

However, these statutory provisions offer limited preventive protection. It is therefore strongly recommended to include detailed confidentiality clauses in technology sourcing agreements, covering the definition, scope, duration, and permitted disclosures of confidential information. Contractual penalties may be agreed in case of breach.

Note: The EU Trade Secrets Directive (2016/943) 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?

Yes. The Swiss Federal Act on Data Protection (FADP) and its Ordinance (OFADP) govern the processing of personal data, including in the context of technology services contracts.

Where the provider qualifies as a processor, the following key requirements apply:

- Processing by a processor must be based on a contract or statutory basis (Art. 9 FADP). Although Swiss law is less prescriptive than the General Data Protection Regulation (GDPR) on form and content, the arrangement should be documented in a written data processing agreement (DPA) defining processing scope, purposes, instructions, security measures, sub-processors, assistance duties, audit or information rights, return/deletion and incident notification.
- The provider may process personal data only for the purposes and within the limits authorised for the customer, and strictly in accordance with the customer's instructions.
- Processing must not violate any statutory or contractual duty of confidentiality.
- The customer must ensure that the provider implements appropriate technical and organisational measures in line with Art. 8 FADP and the OFADP, ensuring

confidentiality, integrity and availability of data, based on risk, processing type, and state of the art.

- For cross-border transfers to countries without an adequate level of protection, appropriate safeguards must be implemented, commonly the EU Standard Contractual Clauses (SCC) with Swiss adaptations. A transfer risk assessment/Transfer Impact Assessment (TIA) is expected in practice where safeguards are relied upon and foreign law may undermine their effectiveness.

As the controller remains liable for data breaches by the processor, it is common practice not to cap liability for data protection violations or regulatory breaches in sourcing agreements.

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

Yes. Under Art. 16 ff. FADP, personal data may be transferred abroad if the recipient country ensures an adequate level of protection, as recognised by the Federal Council. If not, the controller must implement appropriate safeguards, such as:

- EU SCC with Swiss addendum;
- Binding Corporate Rules (BCR); or
- data subject consent or another exception under Art. 17 FADP.

Although Schrems II is not binding in Switzerland, it affects SCC-based transfers. A TIA is recommended. No prior notification to the Federal Data Protection and Information Commissioner (FDPIC) is required under the revised law.

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

Yes. The FADP requires appropriate technical and organisational measures to ensure data security. In addition, sector-specific regulations apply, particularly in finance (FINMA), telecommunications, and healthcare.

The Information Security Act (in force since 1 January 2024) applies to federal authorities as well as to critical infrastructure in the private sector.

In case of data breaches:

- Controllers must notify the FDPIC without undue delay.
- FINMA-supervised institutions must notify FINMA of cyberattacks of substantial importance within the regulatory timeframes and expectations applicable to their sector.
- Since 1 April 2025, operators of critical infrastructures subject to the reporting obligation must report qualifying cyberattacks to BACS within 24 hours of discovery and complete the report within the statutory period.

For the broader private sector, information security is driven by the FADP, contractual commitments, tort and corporate governance duties, sector-specific requirements and recognised standards such as ISO/IEC 27001.

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?

Potentially, yes. Art. 333 CO applies if a business or part of a

business is transferred and retains its identity. An outsourcing transaction may trigger Art. 333 CO, but outsourcing as such does not automatically do so. Where Art. 333 CO applies, employment relationships transfer automatically to the acquirer unless the affected employee objects.

Key features of the transfer:

- The previous employer must inform or consult with employee representatives or employees in due time (Art. 333a CO).
- Employment contracts transfer essentially on existing terms, including accrued entitlements and collective agreement benefits.
- The acquirer may later adjust employment terms (subject to limitations – see question 7.5).
- The transferor and acquirer are jointly and severally liable for claims due prior to transfer or until lawful termination following objection by the employee.

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

There are no statutory disclosure obligations specific to outsourcing. However, the following principles apply:

- Before the transfer, information shared with the acquirer must follow the data minimisation principle and should be limited to anonymised or aggregated data where possible (e.g. roles, functions, seniority, salary bands, notice periods). Disclosure must comply with data protection law.
- At the time of transfer, the acquirer must receive all information necessary to fulfil its duties as the new employer, including individual employment contracts, accrued entitlements, and benefit obligations.

A staged and compliant disclosure process should be agreed in the sourcing agreement.

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

Swiss law does not contain an absolute prohibition on dismissals connected with an outsourcing. However, dismissals intended to circumvent the transfer protection under Art. 333 CO may be challenged as abusive or otherwise unlawful. Ordinary terminations remain possible if notice periods and mandatory law requirements are observed, but the reasons, timing and consultation process require careful assessment.

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

Yes, but only under certain conditions. Material changes require the employee's consent or a "modification termination", i.e. ordinary termination combined with an offer to continue employment on revised terms. The new terms take effect only after the notice period expires. Changes must comply with employment law and must not be abusive or discriminatory.

6.5 Are there any pensions considerations?

Yes. When employees transfer under Art. 333 CO, their vested benefits are moved to the new employer's pension scheme.

Future benefits are calculated according to the new scheme's rules. If the transfer leads to a substantial reduction in the workforce affiliated with the former pension fund, a partial liquidation may be triggered. In such cases, employees may be entitled to a share of free reserves, in addition to their vested benefits.

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

Yes. In offshore outsourcing scenarios, it must be assessed whether Art. 333 CO applies. This provision only governs the transfer of employment if the business unit maintains its identity post-transfer (i.e. continuity of operations, assets, and organisation). If the business is transferred abroad without preserving its structure, no automatic transfer occurs, and employees may face termination.

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)?

Yes. While there is no general outsourcing law in Switzerland, outsourcing in the financial sector is subject to detailed regulation by FINMA and other sector-specific laws.

Key regulatory frameworks include:

- FINMA Circular 2018/3 "Outsourcing – banks and insurers", applicable to banks, securities firms and insurers supervised by FINMA. It sets out requirements on risk assessment, supplier control, business continuity, audit rights, data access and contract content.
- Art. 47 Federal Banking Act (banking secrecy) restricts disclosure of client-identifying information. In outsourcing, the analysis depends on the role of the provider, access arrangements, location, confidentiality controls, client information/consent concepts and FINMA practice; the position should not be reduced to a blanket requirement for explicit consent for every disclosure of non-encrypted data.
- Insurance undertakings must address outsourcing of significant functions under insurance supervisory law and FINMA practice, including business plan implications and regulatory notification or approval requirements where applicable.
- Financial market infrastructures (e.g. stock exchanges, central counterparties, central securities depositories) require prior FINMA approval for outsourcing essential services under the Financial Market Infrastructure Act (FMIA).
- Asset managers, trustees, fund managers and securities firms must comply with the Financial Institutions Act (FinIA) and Financial Services Act (FinSA) when outsourcing, particularly in relation to client data, risk management and information duties.

Outsourcing agreements in regulated sectors must be carefully aligned with supervisory expectations, particularly regarding audit rights, data access, and subcontracting limitations.

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

The most common structure is a master services agreement (MSA) between the customer and an independent service provider, typically covering service scope, governance, pricing and exit terms.

In multi-jurisdictional or group-wide outsourcing, more complex models are used:

- Centralised model: The parent company enters into the MSA and procures services for its affiliates.
- Decentralised model: Each affiliate enters into separate agreements with the provider.
- Hybrid model: Combines central negotiation with local execution via call-off agreements.
- Other structures include:
 - (contractual) joint ventures or partnerships between the customer and provider; and
 - establishment of a captive service entity, often offshore, to provide services exclusively to the group.

The choice of structure depends on regulatory, tax, operational, procurement, data protection, employment, liability and enforceability considerations.

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

Service levels are defined in the Statement of Work and measured against agreed key performance indicators (KPIs). Performance is typically monitored through regular reporting, governance meetings and incident/problem management processes.

If the provider fails to meet the agreed service levels, service credits may be deducted. The amount varies significantly by service criticality, pricing model and negotiation leverage. These credits serve as an incentive and pre-agreed compensation mechanism and provide limited compensation without requiring formal claims.

Service credits are often defined as the sole remedy for the specific failure, but this is typically without prejudice to other rights, e.g. for material breaches or repeated failures, cf. questions 2.4 and 2.7.

Alternatives include bonus/malus schemes or allocating credits to a continuous improvement fund, which may better incentivise long-term performance than punitive deductions.

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

Common pricing models include:

- Cost-plus: Actual provider costs plus a defined margin.
- Fixed price: For stable, predictable services.
- According to usage or volume. Consumption-, unit- or transaction-based pricing, according to users, volumes, transactions, compute/storage usage or other agreed metrics. Time-and-materials pricing, typically for advisory services or termination assistance.

To ensure flexibility and cost control, outsourcing agreements typically include:

- charge variation mechanisms and change management procedures;
- service credits or bonus/malus schemes;

- cost-sharing or gain-sharing models;
- audit rights and benchmarking clauses;
- rules for handling disputed charges; and
- an inflation adjustment mechanism.

The pricing structure should align with service dynamics and incentivise efficiency.

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

Before transferring third-party contracts, the customer must review contractual restrictions given that many contracts prohibit or restrict assignment or require prior written consent from the third party. If a transfer is not permitted, the provider may instead manage the contract on behalf of the customer, or the contract may need to be terminated. If the transfer is allowed without consent, it usually suffices to notify the third party in writing.

Clear documentation and contract-by-contract assessment are essential to ensure legal validity and continuity of service.

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

Key tax considerations in outsourcing transactions under Swiss law include:

- VAT: Transfers of assets or services to the provider generally qualify as taxable supplies. If a business unit is transferred as a going concern, VAT applies under the notification procedure.
- Transfer taxes: Corporate income tax, real estate transfer tax, and Federal securities transfer tax may be triggered depending on the assets involved.
- Transfer pricing: Intragroup outsourcing must comply with arm's length principles. Improper pricing may result in deemed dividends or profit shifts.
- VAT leakage: Intragroup services may incur non-recoverable VAT unless mitigated through group taxation.
- Function shifts: A pure transfer of functions without compensation may raise profit allocation issues, though under Swiss practice, such shifts are generally not taxed unless accompanied by assets or risks.

For cross-border outsourcing, coordinated tax planning is essential to avoid double taxation, minimise withholding taxes, and ensure alignment with international transfer pricing standards.

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 the purposes of a smooth roll-out of software updates. The customer must consider:

- Infrastructure and operation: The customer is responsible for hosting, operation, maintenance, and security of the software environment.
- Update and support: Timely access to patches, upgrades, and support from the licensor or third-party agents must be contractually secured.

- Licence scope: Ensure clarity on usage rights (e.g. per user, device, location), sublicensing, backup rights, and duration.
- Licence compliance: The customer must manage licence audits, ensure adherence to permitted use, and avoid over-deployment.
- Data protection and access: Unlike cloud models, the customer controls all data storage and must ensure appropriate safeguards under applicable law.

On-premise models require greater internal IT capacity but offer more control over data and customisation.

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

Key points include:

- Access control: Limit provider access and implement security measures (e.g. authentication, monitoring).
- Data protection: Conclude a DPA, include SCCs if needed, and minimise personal data exposure.
- Confidentiality: Secure NDAs with the provider and its staff.
- Service levels: Define scope, response times, and escalation in a support agreement.
- Update management: Set rules for patches and coordination.
- Exit: Plan for documentation and handover at contract end.

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?

Software escrow agreements are recognised and enforceable under Swiss law, including in the event of the licensor's insolvency, provided the agreement is properly structured and the escrowed source code is clearly segregated.

However, escrow arrangements are not common practice in Switzerland. Many customers forgo them due to cost or doubts about their ability (or that of third parties) to effectively use the source code once released. That said, escrow can still be valuable in critical systems or bespoke software scenarios to mitigate lock-in risks.

9 Cloud Computing Services (including SaaS)

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services (including Software-as-a-Service)?

No, Switzerland does not have cloud-specific legislation. However, cloud procurement is governed by general laws, including the FADP, secrecy obligations (e.g. Art. 320 and 321 Swiss Criminal Code, sector-specific rules), and public procurement law.

While public entities at federal and cantonal level increasingly use cloud services (including from foreign hyperscalers), this trend has sparked legal and political concerns, particularly regarding data sovereignty, confidentiality, and cross-border data transfers.

9.2 What are the key legal issues to consider and address in the contract when procuring a Software-as-a-Service solution (as opposed to or in addition to issues that apply to on-premise solutions)?

Key legal considerations include:

- Business continuity and disaster recovery: Contractual assurances regarding uptime, redundancy, and recovery times.
- Information and data security: Compliance with the FADP, sector-specific rules, and implementation of appropriate technical and organisational measures.
- Data localisation and cross-border transfers: Ensuring lawful transfers under Art. 16 ff. FADP (e.g. SCCs, TIA, hosting in Switzerland/EU).
- Data portability and exit management: Clear obligations for data return, deletion, and migration support to avoid vendor lock-in.
- Professional secrecy: Guarantees that the provider and its subcontractors respect statutory confidentiality obligations (e.g. Art. 321 Swiss Criminal Code for medical/legal data).
- Audit and control rights: Right to audit or obtain third-party certifications to verify compliance.

10 Artificial Intelligence

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI systems?

No. To date, Switzerland has not yet adopted specific legislation governing AI. Given the rapid evolution of the field and Switzerland positioning itself as an AI innovation hub with strong research institutions, private sector leadership, and public-private initiatives, the Federal Council is taking a very cautious approach. Switzerland signed the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) of the Council of Europe on 27 March 2025 and is preparing to adapt its legal framework accordingly, in particular regarding transparency, data protection, supervision, anti-discrimination, and sector-specific regulation. The Swiss government has given instructions to develop draft legislation implementing the Convention's requirements by the end of 2026.

Switzerland is not bound by the EU AI Act, but the regulation will still have extraterritorial impact on Swiss companies offering AI systems in the EU – similar to the GDPR and EU MDR.

10.2 What rights subsist in the data used to train, test or operate an AI system?

Switzerland has no specific legal framework governing rights in data used to train, test, or operate an AI system.

Furthermore, Swiss law does not recognise ownership of data in the classical sense. While the concept of data ownership is used in practice, it refers to contractual allocation of control and access rights, often termed “economic power of disposal” (*wirtschaftliche Verfügungsmacht*). Although discussed in academic debate, a general right of data ownership has not been adopted by the legislator.

Instead, rights in such data arise from different legal regimes. Copyright under the Federal Act on Copyright and Related Rights may protect data that qualifies as an original

intellectual creation (e.g. texts or images). Where personal data is involved, the FADP applies. Proprietary datasets may also be protected under the Swiss Unfair Competition Act.

In practice, contractual arrangements play a central role in regulating access to and use of data. Overall, Swiss law follows a fragmented approach, and the use of data for AI purposes must be assessed on a case-by-case basis.

10.3 What are the key legal issues to consider and address in the contract when procuring an AI system or AI enabled services (as opposed to or in addition to issues that apply to non-AI software)?

Procuring AI systems under Swiss law requires addressing risks beyond standard IT contracts. The FADP is technology-neutral and therefore applies to AI. Whenever personal data is processed in developing or using an AI system or AI-enabled service, all general data protection principles and obligations must be observed. Uncertainty about how such systems may use inputs makes it essential that contractual provisions on data use be both forward-looking and clear, particularly when many individuals within a large institution access the system or service. IP clauses should define ownership of AI-generated outputs and address infringement risks. Finally, contracts should clearly allocate liability, particularly for inaccurate, biased, or harmful outputs.

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

Swiss IP law is based on human authorship and inventorship. Purely machine-generated outputs will generally not qualify for copyright protection, and an AI system cannot be named as an inventor. This does not mean that AI-assisted developments are unprotectable. Protection may arise where a natural person makes a sufficient creative or inventive contribution, for example, by designing the system, selecting or preparing training data, defining the problem, controlling the generation process, evaluating results and recognising the invention. Ownership is then determined under the ordinary rules of copyright, patent, employment and contract law. The Swiss Federal Administrative Court confirmed in decision B-2532/2024 of 26 June 2025 that an AI system cannot be designated as an inventor. At the same time, the decision indicates that a natural person involved in the AI process and recognising the AI-generated solution may, depending on the circumstances, be named as an inventor. Contracts should therefore allocate rights in AI-assisted models, improvements, outputs and related know-how expressly, rather than relying on default IP rules rejected.

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 that specifically regulate the procurement of blockchain-based solutions. However, Switzerland has introduced DLT-specific legislation that governs the issuance and transfer of tokenised rights (e.g. register-based uncertificated securities) and sets regulatory requirements for DLT trading facilities.

While procurement as such remains unregulated, use cases involving financial instruments, personal data, or critical infrastructure may trigger regulatory obligations.

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

The most visible adoption in Switzerland is in financial services and fintech, including tokenisation, crypto-asset custody and trading, digital securities and related market-infrastructure projects. The Zug region, often referred to as “Crypto Valley”, remains an important hub for blockchain and crypto ventures. The DLT legislation, in force since 1 August 2021, introduced a framework for register-based uncertificated securities, DLT trading facilities and the segregation of certain crypto-assets in insolvency.

Other use cases exist in supply chain management, logistics, energy trading, decentralised energy systems, digital identity, certification and provenance solutions, although adoption outside financial services is more use-case specific and less uniform.

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

Key legal challenges arise from the decentralised, immutable and transparent nature of blockchain. In public (permissionless) blockchains, it may be unclear who qualifies as the data controller, complicating compliance with data protection laws. Further, the immutability of data can conflict with the data accuracy principle, especially if personal data must be corrected or deleted.

To mitigate these issues, companies often use private (permissioned) blockchains to control access and allow for data management, store personal data off-chain, with only hash values on the blockchain, and apply encryption, where decryption keys are accessible only to authorised individuals.

12 Looking Ahead

12.1 Looking ahead, what technological or legal development which is likely to occur in the next five years poses the biggest challenge for technology procurement, and how should businesses prepare for it?

Over the next five years, the most significant challenge for technology procurement will not be one single regulation, but the convergence of AI governance, cyber resilience, cloud concentration risk and digital sovereignty. Procurement decisions will increasingly be assessed not only by reference to

functionality, price and service levels, but also by reference to control, resilience, regulatory auditability and the legal environment in which the relevant technology stack operates.

Cybersecurity and operational resilience are becoming core procurement requirements. Switzerland has introduced mandatory cyberattack reporting for operators of critical infrastructure and is preparing rules on the cyber resilience of digital products. In the EU, frameworks such as the Digital Operational Resilience Act, the Cyber Resilience Act, NIS2 and the Data Act are raising expectations regarding third-party technology risk, incident handling, portability, interoperability and exit capability. Even where these regimes do not apply directly to a Swiss customer, they will increasingly shape market practice, supplier documentation and contractual standards.

Cloud procurement will remain particularly sensitive. Dependence on a small number of global hyperscalers creates legal, operational and strategic risks, including concentration risk, vendor lock-in, cross-border access risks, sanctions exposure, limited bargaining power and uncertainty regarding effective control over data and infrastructure. These risks cannot be eliminated by contractual clauses alone. They must be addressed through architecture, governance and sourcing strategy.

AI will add a further layer to this development. Switzerland is preparing to implement the Council of Europe AI Convention, while Swiss businesses with EU-facing activities may also fall within the scope of the EU AI Act. In procurement practice, this will increase the need for clear contractual provisions on permitted data use, model governance, transparency, output monitoring, human oversight, auditability, IP and liability. AI should therefore not be treated as an isolated software feature, but as a regulated and risk-relevant component of the broader technology stack.

Businesses should prepare by treating technology procurement as a strategic risk-management function. In practical terms, this means: conducting regulatory and geopolitical due diligence before supplier selection; classifying data, systems and use cases by criticality; requiring transparent subcontracting and data-transfer structures; negotiating robust audit, incident notification, security, portability and exit rights; avoiding unnecessary technical lock-in; using encryption and key-management models under appropriate customer control; and establishing internal governance for AI systems and critical digital services throughout their lifecycle.

The future of technology procurement will therefore be shaped by a shift from “buying technology” to governing technological dependency. Successful customers will be those that can demonstrate not only that a solution works, but that it remains lawful, secure, explainable, portable and resilient under changing regulatory, geopolitical and operational conditions.



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*. She 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 more than 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 combines in-depth knowledge on complex contractual matters in outsourcing and information technology projects with the experience of implementing such global projects as in-house lawyer.

Martina studied law, philosophy and political science at the University of Bern where she graduated in 1996 (*magna cum laude*), passed the Bar in 1999 with excellence and received an LL.M. from the 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
Hornbachstrasse 22
8008 Zürich
Switzerland

Tel: +41 44 201 66 11
Email: martina.arioli@arioli-law.ch
LinkedIn: www.linkedin.com/in/martina-arioli-ab809b1

Arioli Law is a leading boutique law firm established in 2013 in the heart of Zurich. It was one of the first one-woman, pure technology law firms in Switzerland. Our attorneys are committed to providing excellent services to our clients in a wide range of industries and the public sector. We believe that hands-on work by highly specialised and experienced partners leads to better and faster results at lower costs to our clients. The renowned Swiss business magazine BILANZ has ranked Arioli Law amongst the Switzerland's top law firms in TMT and IP law since the first ranking issued in 2017. Our attorneys have garnered rankings and awards including *Chambers*, *The Legal 500*, *Leaders League* and *Who's Who Legal*.

www.arioli-law.ch

ariolilaw



The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Technology Sourcing 2026 features two expert analysis chapters and 19 Q&A jurisdiction chapters covering key issues, including:

- Procurement Processes
- Contracting Issues
- Dispute Resolution Procedures
- Intellectual Property Rights
- Data Protection and Information Security
- Outsourcing of Technology Services
- Software Licensing
- Cloud Computing Services (including SaaS)
- Artificial Intelligence
- Blockchain