

Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top ranked lawyers

Outsourcing

Switzerland
Niederer Kraft Frey

[chambers.com](https://www.chambers.com)

2019

Law and Practice

Contributed by Niederer Kraft Frey

Contents

1. Outsourcing Market	p.3
1.1 IT Outsourcing	p.3
1.2 New Technology	p.4
2. Regulatory and Legal Environment	p.5
2.1 Legal and Regulatory Restrictions on Outsourcing	p.5
2.2 Industry Specific Restrictions	p.6
2.3 Legal or Regulatory Restrictions on Data Processing or Data Security	p.6
2.4 Penalties for Breach of Such Laws	p.7
2.5 Contractual Protections on Data and Security	p.7
3. Contract Models	p.8
3.1 Standard Supplier Customer Model	p.8
3.2 Alternative Contract Models	p.8
3.3 Captives and Shared Services Centres	p.8
4. Contract Terms	p.9
4.1 Customer Protections	p.9
4.2 Termination	p.9
4.3 Liability	p.10
4.4 Implied terms	p.10
5. HR	p.11
5.1 Rules Governing Employee Transfers	p.11
5.2 Trade Union or Workers Council Consultation	p.11
5.3 Market Practice on Employee Transfers	p.11
6. Asset Transfer	p.11
6.1 Asset Transfer Terms	p.11

Niederer Kraft Frey (Zürich), established in 1936, is a pre-eminent Swiss law firm with a proven track record of legal excellence and innovation. Throughout its history, the firm has continuously worked on the most important and demanding cases entrusted to Swiss law firms. Lawyers work and think internationally. As a market leader in Switzerland, the firm has built long-standing relationships with the world's best international law firms. The firm currently employs around 100 lawyers, including 35 partners

(as per 1 January 2018). Together with our administrative staff of around 70 people, this adds up to approximately 170 employees. Its offices are located on Bahnhofstrasse in the heart of Zurich's banking and financial district. Niederer Kraft Frey is a stock corporation (Aktiengesellschaft) with a board of directors composed of all partners of the firm. In its non-assignment-related business, the firm is managed by an executive committee of five partners headed by the managing partner.

Author



Dr Andrés Gurovits specialises in technology, corporate and dispute resolution, specifically arbitration, with a particular focus on technology, sports and corporate matters.

1. Outsourcing Market

1.1 IT Outsourcing

Outsourcing vs. insourcing

Both the IT and BP outsourcing markets in Switzerland are currently characterised by opposing trends. On the one hand, the traditional proponents of outsourcing continue to emphasise the classic advantages of outsourcing, namely cost and quality benefits. On the other hand, however, an important group of insourcers has recently established themselves and have critically assessed the effects of outsourcing, initiating steps to reintegrate outsourced business areas.

The traditional arguments pro outsourcing

The traditional proponents of outsourcing in Switzerland are supported by empirical studies, such as a study by PwC in January 2018 that confirms the relevance of the topic for the financial sector at least. Accordingly, large Swiss financial service providers have significantly expanded their outsourcing expenditures and outsourced IT and business processes. According to PwC, the focus was on various outsourcing centres in Eastern and Central Europe. In addition to IT, the business areas affected by outsourcing are primarily back-office functions such as internal audits, human resources, risk management and compliance, as well as operations. The most important drivers for outsourcing are said to be savings potentials of up to 60%, which could be realised primarily due to the large differences in wage costs and quality gains.

New trend towards insourcing?

The NZZ am Sonntag (a Swiss Sunday newspaper), on the other hand, reported in its issue of 27 May 2018 on the new insourcing strategy of a major Swiss bank that is pursuing a strategy of strengthening Switzerland as a business location.

According to NZZ am Sonntag, the workforces of the big banks have been shrinking for years, but the latest personnel statistics of that major Swiss bank (UBS) show an impressive turnaround. In the first three months of 2018, it hired 1,200 additional employees, and the workforce has grown by more than 3,000 since the beginning of 2017. In its quarterly report, the bank states that the reason for this recruitment boom is insourcing. UBS is recovering many of the activities that it had outsourced to external suppliers, thereby cutting 1,500 external jobs since the beginning of 2018, according to NZZ am Sonntag, although the bank continues to employ 24,000 external staff.

Interestingly, the bank also cites quality considerations as a reason for insourcing. While quality has been one of the main drivers of outsourcing alongside costs for many years, it is now cited as one of the reasons for insourcing. The bank also stated that it wanted to retain its strategic IT expertise. Finally, shorter communication channels and better efficiency were decisive for the insourcing decision.

Reported shortcomings of outsourcing

This raises the fundamental question of whether the quality improvements that were expected in many places could not be achieved by outsourcing. Experts surveyed by NZZ am Sonntag report that companies are moving away from the classic outsourcing strategy because quality is often lacking and implementation takes too long. There are even reports of cases in which the interfaces to the external provider did not work properly, so that a second internal department has to be created parallel to the outsourced area, which led to the original cost savings being cancelled out.

Complaints from Swiss bank employees about the poor service of outsourced tasks are accumulating, particularly in the

sensitive personnel area. The frequent change of contact persons and their insufficient language skills are also criticised. Also, technical errors can have far-reaching consequences. On 3 May 2018, the business magazine Bilanz reported that a large number of invoices had not been paid at Credit Suisse. The bank had outsourced its creditor management, including accounts payable management, to India at the end of 2017, with unpleasant consequences: because of an internal error, a large number of invoices were not paid. The problem could be solved in the meantime but, as the incident suggests, outsourcing can also lead to undesired results.

Furthermore, a trend reversal is foreseeable not only in terms of quality, but also in terms of costs. In the classic outsourcing countries such as Poland or India, for example, the salaries of skilled workers are reported to have risen sharply. According to NZZ am Sonntag, about 250,000 people now work in Poland's financial industry, carrying out administrative office and IT work for major western corporations. UBS and Credit Suisse are also prominently represented, each with around 4,000 employees. According to industry experts, there is already a shortage of qualified employees. The consequences are strong wage increases and an enormously high fluctuation rate, which in many places exceeds 20%.

In light of the above flaws, it is not surprising that companies are increasingly considering insourcing. According to NZZ am Sonntag, new possibilities of digitisation whereby repetitive actions can now be automated (and require specific new skills from employees) also play a role in these considerations. Accordingly, repetitive activities can now be automated.

Important insights for managers

The trade journal Computerworld examined the advantages and disadvantages of outsourcing in detail, primarily in IT, and published the results in its report in 2017. According to the journal, outsourcing is still a trend, but management is often dissatisfied with the results.

According to Computerworld, outsourcing remains a reasonable option to save costs, in principle. The current IT outsourcing market in Switzerland is still estimated at around CHF3 billion, and the trend is still rising. The reasons for this are well-known: reducing costs, focusing on core business and purchasing specialist knowledge. However, it is clear that these advantages can only be achieved if goals are realistically defined and implementation is ensured with appropriate measures.

However, there is often a lack of prudent planning, especially in the area of implementation. On the one hand, this is due to the fact that outsourcing providers do not know enough about the requirements of the business. On the other hand, it is due to the fact that the companies lack internal IT exper-

tise as they have outsourced or dismissed all IT employees in order to save costs. The study has shown, however, that a minimum number of key personnel must always remain in the company in order to avoid being completely at the mercy of the outsourcing provider. It must therefore always be the maxim of the outsourcing company never to outsource all its competencies. According to the study by Computerworld, companies must also consider that outsourcing may often pay off quite well in theory, but in the medium term the complexity increases and costs arise where none are expected. Finally, both the customer and the provider must avoid exaggerated expectations on both sides, which may be the result of poor communication and the main cause for this dissatisfaction. Against this background, it is absolutely key that the outsourcing provider does not hide behind his or her technical jargon, but always clarifies what the customer wants exactly. As the Computerworld study suggests, customers and providers still do not speak the same language, which often leads to disappointed expectations on the part of customers who, due to poor communication, make demands that go beyond what has been specifically agreed in the contract.

Conclusion

In summary, two opposing tendencies can be observed today. On the one hand, companies have begun to say goodbye to a comprehensive outsourcing strategy and to reintegrate important IT and/or business processes. On the other hand, outsourcing can still be effective today, especially when customers realistically define their goals and expectations, when providers really understand their customers' goals and expectations, and when, in principle, clients and contractors communicate openly and fully align their goals. If there is a reasonable win-win situation for both parties, then the outsourcing project still has good prospects of successful implementation. The lawyers advising the parties play an important role here, ensuring that the parties speak the same language and understand what is to be agreed in the outsourcing contract.

1.2 New Technology

According to relevant market sources, the digital transformation is and will remain the focus of IT managers in 2018. This will also influence the outsourcing market, because many companies cannot provide the necessary resources for a successful digital transformation internally and therefore have to outsource the corresponding developments.

According to a study by International Data Group (IDG), approximately 35% of IT budgets nowadays is spent on building new digital business models. Consequently, it is not a question of whether companies tackle the digital transformation, but rather how and at what speed.

Central to the digital transformation are (i) big data/analytics, (ii) artificial intelligence (AI), (iii) the Internet of Things

(IoT), (iv) IT security, (v) software development and (vi) cloud solutions.

Big data/analytics

Big data/analytics (the real-time analysis of large amounts of structured and unstructured data) is an indispensable tool for the implementation of digital transformation and the development of IoT solutions. According to the IDG study, about 70% of all IoT applications use big data/analytics methods to gain information and ultimately create benefits for companies and customers from raw data. According to the author's own experience, there is still a great lack of skills among companies that plan to implement and roll-out IoT solutions, which they primarily counter with the sourcing of corresponding services.

IoT/artificial intelligence (AI)

The Internet of Things plays the role of a catalyst in digital transformation. According to the IDG study mentioned above, the International Data Corporation (IDC) expects the number of networked devices worldwide to increase to more than 22 billion in the foreseeable future. This in turn will result in the development of approximately 200,000 new apps and solutions that will benefit and be based, at least partly, on AI. The boost of the roll-out of IoT solutions further reinforces the already enormous importance of IT security (see below).

IT security

The growing demands on IT security and cybersecurity are also influencing developments in the sourcing markets. The growing influence of IoT solutions reinforces expectations for comprehensive cybersecurity measures. Big data/analytics and AI are also used in this environment, in that these approaches are applied to predict and avoid possible future attacks, or to reduce their consequences. The constantly increasing importance of IT security is also driven by the continuing increase in technological penetration and networking. The "always on" approach, according to which everyone can be reached online at any time and anywhere, requires IT managers to make appropriate solutions available; due to a lack of skilled personnel, however, this can often only be provided by outsourcing or purchasing appropriate security services. In addition, security-as-a-service (SaaS) solutions are becoming increasingly important, and create tempting alternative solutions for IT departments.

Software development

Another factor shaping or enabling the digital transformation is the increased expansion of software development capacities and their sourcing/purchasing if internal development resources are insufficient. According to IDG, the ability to develop new strategic apps and services will be critical to a company's successful digital transformation.

IDG expects that by implementing alternative approaches, such as agile or Scrum technologies on the developer side, and DevOps methods on the operational side, businesses can carry out their software development projects faster and with better quality. As many businesses lack sufficiently skilled personnel, relevant services must be sourced from specialised providers.

IDG also expects that the currently prevailing monolithic software structures, such as those found in ERP solutions, for instance, have survived, and that SaaS will prevail as the dominant delivery method of software.

Cloud

Moreover, Application Programming Interfaces (API) that enable connecting to large cloud platforms and to interweave external cloud services with internal processes will continue to gain in importance. In a world that is increasingly networked by IoT solutions and mobile devices, the volume of data is constantly growing, and this trend further increases the demand for cloud-computing-based services such as IaaS or PaaS. According to IDG, in 2018 at least half of IT spending flows into cloud-based solutions.

2. Regulatory and Legal Environment

2.1 Legal and Regulatory Restrictions on Outsourcing

Swiss law does not provide for specific outsourcing-related provisions that would apply across all markets. Outsourcing-related statutory and regulatory restrictions can be found in (i) the Outsourcing Circular of the Swiss Financial Market Supervisory Authority, (ii) federal, cantonal and communal provisions on the public procurement of goods and services, and (iii) the Swiss Federal Telecommunications Act.

Outsourcing in the Financial Markets

The Swiss Financial Market Supervisory Authority (FINMA) publishes the so-called Circular on outsourcing for banks and insurance companies (Outsourcing Circular); the latest version came into effect on 1 April 2018. FINMA issued the Outsourcing Circular on the basis of, inter alia, the Swiss Federal Banking Act and the Swiss Federal Act on Surveillance of Insurers, which both give FINMA the competence to supervise the organisation and operation of banks and insurers. See **2.2 Industry-Specific Restrictions** for discussion of the Outsourcing Circular and the limitations under the Swiss Federal Banking Act on the disclosure of information abroad.

Public Procurement

Public authorities on a federal, cantonal or communal level need to procure services by tender, including outsourcing services, if a certain threshold amount of the contract value

is met. The current threshold amount on the federal level, for instance, is CHF230,000.

Telecommunications Act

If telecommunications services are outsourced (eg, the WAN and voice connections) within a group of undertakings on a country- or even world-wide basis, the provider will have to respect the secrecy obligations under the Swiss Federal Telecommunications Act, according to which anyone who is providing a telecommunications service must refrain from disclosing any information relating to its customers' communications to third parties, and from giving anyone else the opportunity to do so.

2.2 Industry Specific Restrictions

The Outsourcing Circular

The Outsourcing Circular mentioned above defines the supervisory requirements for banks, securities dealers and insurance companies in Switzerland, in terms of proper organisation and risk management. As a rule, banks, securities dealers and insurers are permitted to outsource IT and business functions, subject to the limitations set out in the Outsourcing Circular (and applicable law). For instance, according to the Outsourcing Circular, they are not permitted to outsource strategic management, supervision and control as well as business functions that involve strategic decision-making.

The Outsourcing Circular also sets out the conditions for the following:

- the selection, instruction and control of the outsourcing provider;
- outsourcing within a group of undertakings;
- the responsibility of the bank or securities dealer vis-à-vis FINMA;
- security;
- audit and supervision by FINMA;
- outsourcing to another country; and
- requirements under the outsourcing contract.

Swiss Banking Secrecy

Even if banks and securities dealers are, in principle, permitted to outsource to an outsourcing provider in Switzerland or abroad, in accordance with Article 47 of the Banking Act on banking secrecy they would not be permitted to transmit non-anonymised or unencrypted data to a site outside Switzerland.

See **2.3 Legal or Regulatory Restrictions on Data Processing or Data Security** for discussion of other data-related topics.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

The Swiss Data Protection Act and the Implementing Ordinance

The processing of personal data in Switzerland must comply with the provisions under the Swiss Federal Data Protection Act (DPA) and the implementing Ordinance. Principles under the DPA are quite comparable with those under data protection laws in the EU and EEA. The European Commission has issued an adequacy decision in respect of Swiss data protection law, thus facilitating, in particular, the flow of personal data between EEA countries and Switzerland. While the General Data Protection Regulation (GDPR) became applicable in May 2018, the contemplated revision of the Swiss DPA is still under discussion by Swiss parliament and it is not yet known whether or when the revised law will come into effect in Switzerland.

The so-called outsourcing privilege

Under the current DPA, companies are entitled, in principle, to outsource the processing of personal data on the basis of a contract, provided there are no specific statutory or contractual obligations that would prohibit the outsourcing, and provided that the customer ensures that the outsourcing provider (processor) will process the data in a way the customer itself is permitted to do. Unlike Article 28 GDPR, the Swiss DPA does not set out in detail the subject matters that must be covered in an outsourcing contract.

Trans-border data flow

If personal data is to be transferred as part of an outsourcing arrangement to a country that does not have legislation in place that would ensure an adequate level of data protection, relevant safeguards must be put in place before the data transfer starts. Such safeguards would include (apart from obtaining each data subject's explicit consent, which is usually an unrealistic option) putting in place a contractual arrangement that is based on either the model clauses issued by the Swiss Data Protection and Information Commissioner (FDPIC) or the model clauses issued by the EU Commission. In respect of US-American providers, a data transfer could be permissible under the Swiss-US privacy Shield framework.

Appropriate organisational and technical measures

According to the DPA, all companies processing personal data must implement effective organisational and technical measures to ensure an appropriate level of security for the data. This also applies under an outsourcing framework, and the customer will have to satisfy him or herself that the provider is in compliance with this requirement. The Implementing Ordinance on data protection describes in more detail the measures that a data controller or data processor must put in place. In accordance therewith, the relevant systems must be appropriately protected against the following risks:

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use; and
- unauthorised alteration, copying, access or other unauthorised processing.

When designing and implementing the technical and organisational measures, controllers and processors must properly take the following into account:

- the purpose of the data processing;
- the nature and extent of the data processing;
- the potential risks that the data processing may create for the data subjects; and
- the current state of the art.

These measures must be reviewed periodically.

The Implementing Ordinance also requires the controller or processor to put in place specific measures regarding the following in particular:

- entrance control (ie, unauthorised persons must be denied the access to facilities in which personal data is being processed);
- personal data carrier control (ie, unauthorised persons must be prevented from reading, copying, altering or removing data carriers);
- transport control (ie, the disclosure of personal data and the unauthorised reading, copying, alteration or deletion of data must be prevented during the transport of data carriers);
- disclosure control (ie, data recipients to whom personal data is disclosed by means of devices for data transmission must be identifiable);
- storage control (ie, unauthorised storage and the unauthorised knowledge, alteration or deletion of stored personal data must be prevented);
- usage control (ie, the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented);
- access control (ie, access by authorised persons must be limited to the personal data that they require to fulfil their task – in other words, disclosure on a need-to-know basis only); and
- input control (ie, in automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by whom).

2.4 Penalties for Breach of Such Laws

Banking Act

A wilful violation of banking secrecy obligations is subject to criminal sanction (imprisonment of up to three years or a fine). Anyone who negligently violates the banking secrecy obligations is subject to a fine of up to CHF250,000.

Data Protection Act

Under the DPA, anyone who violates the data subjects' right of information by wilfully providing false or incomplete information can, on the request of the data subject, be sanctioned with a fine of up to CHF10,000. In addition, anyone who (i) fails to inform the FDPIC about the safeguards taken if personal data is to be transferred to a country whose data protection legislation does not provide an adequate level of protection, or (ii) fails to notify the FDPIC about the processing of data files containing sensitive personal data (subject to exceptions provided for in the law), or (iii) provides the FDPIC with false information in the course of an investigation, or refuses to co-operate in such, shall be subject to a fine of up to CHF10,000. These latter cases would be prosecuted *ex officio* – ie, no complaint of the data subjects would be required.

Telecommunications Act

Under the Telecommunications Act, anyone providing a telecommunications service shall be liable to imprisonment of up to three years or a fine if he or she falsifies or suppresses information, gives any third party the opportunity – or instigates a third party – to do so. Further, anyone who intercepts private communication by using telecommunication devices and uses the information for himself or discloses it to third parties without permission can be sanctioned with imprisonment of up to one year.

2.5 Contractual Protections on Data and Security

As a matter of customary practice, outsourcing contracts distinguish between (i) (general) confidentiality, (ii) data protection, and (iii) data security obligations.

General confidentiality obligations

Confidentiality provisions deal with the disclosure and non-disclosure of the parties' confidential information, which may comprise personal data as well as non-personal data, such as know-how, trade secrets, IP, machine-data processed in IoT applications, processes, handbooks and any other similar types of information that the discloser wants, and has a legitimate reason, to keep protected. Usually, the recipient of the information agrees to do the following:

- protect the information and to use at least the same care and discretion to avoid disclosure, publication or dissemination of the discloser's information as it uses for its own similar information that it does not wish to disclose, publish or disseminate;
- use the discloser's information for the purpose for which it was disclosed;
- share the discloser's information within (or, if so permitted, outside) the organisation on a need-to-know basis only; and
- ensure that all further recipients of the information adhere to the confidentiality obligations under the contract.

Data protection obligations

Data protection provisions usually consist of a compliance with law section, and specific rights and obligations applicable between the customer and the outsourcing provider. The compliance with law part obliges the parties to be compliant with applicable laws, particularly data protection laws. The data specific data protection provisions provide a set of obligations (and rights) for the parties, aimed at properly implementing the statutory data protection obligations in the outsourcing structure at hand. As a result of the GDPR, a practice seems to be evolving whereby the parties enter into a specific data protection annex or data protection agreement addressing, in particular, the conditions under Article 28 GDPR on the sub-processing of personal data. Such data processing addendum or agreement should typically address the following areas:

- covenants of the supplier;
- security (which can also be dealt with by referring to a specific data security annex – see below);
- the engagement of sub-processors;
- the rights of the data subjects;
- rights and obligations in case of a data breach;
- the retention and deletion or return of personal data;
- the audit rights of the customer and/or its relevant supervisory authority;
- trans-border data transfers; and
- the keeping of data processing records.

Data security obligations

While the data protection provisions summarised above typically oblige the provider (and customer) to put effective organisational and technical measures in place to provide appropriate security for (personal and confidential) data, data security provisions set out specific technical (and organisational) measures with which the parties will have to comply in the context of their outsourcing arrangement. Specifying these rules is typically a task for the IT and data security experts of the parties, who must be involved in the drafting of the relevant sections of the outsourcing contract. According to a common approach that can be found in the market, the outsourcing contract (or the main body of it) will oblige the provider to obtain and maintain certification according to an accepted standard, such as the ISO/IEC 27001 et seq standard. The provider would also be obliged to undergo regular audits to verify compliance with such standard, and to comply at all times with the conditions and requirements under the agreed standard. Project-specific rights and obligations would then usually be set out in a more detailed annex to the outsourcing contract.

3. Contract Models

3.1 Standard Supplier Customer Model

Parties typically negotiate a master or framework outsourcing contract, under the umbrella of which they agree on service-specific individual agreements or schedules, respectively. The service agreements typically comprise, on the one hand, project-related arrangements such as for the transition and transformation at the beginning of the collaboration and for termination assistance at the end of the collaboration in order to ensure a smooth transition of the outsourced services to the customer or another provider. On the other hand, service agreements are in place for the various services that the provider is to deliver during the outsourcing set-up. Exhibits or annexes complement the master agreement, project agreements and/or service agreements, as the case may be, by addressing particular (technical, organisational or legal) topics in detail.

In cross-border outsourcing, the parties may have to arrange for local agreements (ie, agreements between local (foreign) entities of the customer and provider), for legal, tax and/or technical considerations. This typically adds some complexity to the contractual set-up, as the local agreements are entered into by parties different to those under the master agreement. In such cases, the parties to the master agreement are well-advised to clarify (in the master agreement) that any performance by the local entities or parties to the local entities, respectively, accordingly discharges (or obliges) the parties under the master agreement, and that the parties under the master agreement will ensure that the local entities will abstain from raising any claim against each other on a local level and that any disputes that arise shall be resolved between the parties to the master agreement.

3.2 Alternative Contract Models

The contract model discussed above is by far the most frequently used in Switzerland. Joint venture models can be found in practice, particularly in cases where the parties intend to combine specific know-how and/or financial resources in order to commercialise jointly a service that the customer has outsourced to the provider. This can be found in respect of industry 4.0/IoT solutions, the development of which the customer has (partly) outsourced to the provider, and where the parties have identified opportunities to market that solution on a much wider basis. In such cases, the parties may have a strong business case that would also justify accepting the complexity of the set-up and the costs associated with its set-up and operation.

3.3 Captives and Shared Services Centres

The outsourcing of IT and/or business functions to an affiliate that is controlled by or is under common control with the customer can be found, where the customer may expect significant cost savings. Outsourcing by Swiss companies to captives is, therefore, limited in most cases to the outsource-

ing of business functions (eg, accounting, back-office, internal audit) to an affiliate in a low(er) cost country. The outsourcing of IT functions (by non-IT companies), however, typically makes less sense, as the customer (or the group of companies to which it belongs) would have to build up its own IT know-how (which is not its core business and would be costly) and would not benefit from the economies of scale, expertise and know-how of specialised providers.

4. Contract Terms

4.1 Customer Protections

Service specifications / service fee specifications

For the customer, but also for the provider, it is of utmost importance to manage expectations and to specify precisely the services (and the relevant prices) that the provider shall provide and the customer shall receive. The provider and customer must have a clear common understanding of what the provider is expected to deliver and what the charges will be. This sounds very simple, but in practice it is often very challenging to implement. On the other hand, once a clear agreement has been reached, where both parties have the same expectations in respect of service delivery and price, the foundations have been laid for co-operation, whereby the risk of future conflicts is likely to be much lower.

Service levels

Service levels or service level agreements (SLAs) play an important role when the parties specify the services, as they define the parameters against which the services provided by the provider will be measured. Under-performance by the provider typically triggers service credits (ie, a pre-defined price reduction), to the benefit of the customer.

Service improvement plan

In addition to service credits, under-performance by the provider also typically obliges the provider to investigate the root cause for its failure, and to prepare and present to the customer a plan as to how the deficiencies will be remedied so that the provider will perform properly in the future.

Step-in rights

Should the provider significantly under-perform, so-called step-in rights may also protect the customer, according to which the customer has the right to take over the affected service (or to temporarily engage another provider) until the provider can re-establish proper service delivery. Even if the exercise of a step-in right may prove to be complex in practice, it may still be an appropriate means for the customer to protect its business.

Benchmarking

Benchmarking provisions allow the customer to have service quality and service prices benchmarked over time against the services and charges of other providers. This is particu-

larly relevant for customers who have outsourced for a long period of time and are bound by a long-term contract.

Governance

Practice shows that outsourcing projects can fail or be delayed if the provider changes project teams and replaces personnel who have become familiar with the customer's environment with new project members who have to start from scratch. Such changes may cause serious disruptions in the transition/transformation phase, and also during service delivery. Therefore, governance provisions under outsourcing agreements often set out clear rules that must be followed if and when a provider intends to replace its service personnel, particularly those employees who are considered to be "key" for service delivery. Governance provisions also deal with escalation processes in case of disputes. In the case of a serious incident, it is of utmost importance to the customer that the provider reacts quickly. If there is a dispute regarding the root cause or the measures to cure the incident, the dispute should be quickly escalated to higher levels of management, who would then solve the issue pragmatically not only by considering the recriminations, but by applying a more holistic approach that takes into account the entire customer-provider relationship. If properly drafted, such governance clauses usually contribute to the protection of the customer's interests.

Performance or parental guarantee

Under a parental guarantee, the (ultimate) mother company of the Swiss provider commits itself to guarantee the performance of its subsidiary. This may be particularly relevant where the Swiss entity that contracts under the master agreement is small in terms of financial strength and staff. If properly drafted, such an instrument also allows the customer to draw the guarantee and the amounts committed therein in the case of a serious breach by the provider, without having to fight the dispute through all instances.

4.2 Termination

Contracts governed by Swiss law distinguish between termination for convenience, termination for cause, and withdrawal from the contract.

Termination for convenience

In the case of termination for convenience, a party (typically the customer) terminates the contract when no (serious) dispute has arisen. The customer either terminates if the contract has reached the agreed term (either the initial term or, if the contract so provides, a renewed term), or terminates the contract prior to the agreed term, but only if the contract expressly provides the customer's right for early termination for convenience. If the contract provides for such, the customer will typically be obliged to pay a specified termination fee.

Termination for cause

In the case of termination for cause, the non-breaching party may terminate the contract if the other party has committed a material breach of the contract and, if the breach is remediable, has not remedied the breach within a specified grace period. Termination for cause is typically also expressly permitted if the other party becomes subject to bankruptcy (or similar) proceedings, or ceases to do business. Where the particularities of the case so require, change of control can also be a reason for termination for cause.

Withdrawal

In contrast to termination where the agreement ceases to exist (*ex nunc*) if and when the termination has become effective, withdrawal from the contract means retroactive termination of the contract (*ex tunc*), which means, in essence, that the parties are put in a position as if the contract had never been in effect. Withdrawal of the contract by the customer is typically the *ultima ratio* if the provider is not able to take over service delivery properly and effect a successful transition or migration, respectively. In such cases, the provider will have to reimburse the customer all amounts paid, and may also become liable for compensation of damages.

4.3 Liability

Direct and indirect damages

Swiss law does not distinguish between direct and indirect damages. According to Swiss law, a party that breaches a contract becomes, in principle, liable to compensate the non-breaching party for all damages incurred by the latter, that he or she can properly establish. However, Swiss law also allows the parties to limit/exclude liability in advance, except, as a rule, for wilful misconduct or gross negligence.

Market practice

The above notwithstanding, many outsourcing contracts provide for a different regime for direct damages and indirect damages. In such cases, the provider typically accepts a higher liability for direct damages than for indirect damages. Given that the law itself does not provide a distinction between direct and indirect damages, nor a definition thereof, relevant court practice would have to be consulted if a dispute arose. As a rule, damages that are more linked to a damaging act are direct damages, while others would qualify as indirect damages. If, for instance, an employee of the provider damages a customer's server, the cost to repair the server would be a direct damage, but the loss of profit caused by the server being down would typically be considered an indirect damage. The more appropriate option for the parties, however, would be to define in the contract what the parties consider, under the particularities of the outsourcing model at hand, to be direct and indirect damages, thus providing guidance that would also bind the courts if the dispute is not resolved amicably.

According to market practice, providers typically intend to exclude liability for indirect damages and to limit liability for direct damages, and customers typically reject an exclusion for indirect damages. In many cases, the parties agree that liability for indirect damages can be excluded or capped at a lower threshold, and that liability for direct damages shall be capped at a higher threshold. Such exclusion/limitation, however, will not apply in case of wilful misconduct or gross negligence (which would anyhow apply by operation of law).

4.4 Implied terms

The Swiss Code of Obligations provides a framework of general principles that applies to all types of contracts, and specific terms that apply in respect of some specific types of contract, such as purchase, lease, employment, work and mandate agreements. Under Swiss law, outsourcing contracts are typically regarded as mixed contracts (combining elements of several specific types of contracts defined in the law) or contracts *sui generis* that do not contain elements of such defined contracts. It is usually difficult for the parties to predict how the courts would qualify an outsourcing contract and what specific provisions they would apply. Therefore, the parties are well advised to provide for sufficiently detailed rules for all contract topics they deem to be relevant for their outsourcing arrangement. Such mutually agreed provisions will usually prevail over the statutory clauses that may (otherwise) be applicable, as most of such statutory provisions are not of a mandatory nature. Only where the law provides for a mandatory provision would the parties not be permitted to deviate from what the legislators had foreseen.

The provisions of the Swiss Code of Obligations regarding lease or rental agreements provide that the lessor is required to make the leased object available on the agreed date in a condition that is fit for its designated use, and to maintain it in that condition. Likewise, the provisions of the Swiss Code of Obligations regarding purchase contracts provide that the seller is liable to the buyer for any breach of warranty of quality, and for any defects that would materially or legally negate or substantially reduce the value of the object or its fitness for the designated purpose. Both provisions state that implied terms on quality are relevant, and both provisions may well become applicable in an outsourcing set-up. The statutory terms on lease agreement may well be relevant in respect of outsourcing agreements providing for housing and/or other elements of lease, such as the lease or usage of IT servers and other infrastructure, for example. The statutory terms on purchase contracts may become applicable, by analogy, in respect of work contracts – ie, under contracts according to which the provider must procure for a specific, pre-defined work result, as would be the case, eg, in outsourcing arrangements where the provider shall ensure certain work results in terms of service levels or similar benchmarks.

5. HR

5.1 Rules Governing Employee Transfers

In accordance with the Swiss Code of Obligations, where the employer transfers a business, or a part thereof, to a third party, the employment relationship and all relevant rights and obligations pass to the acquirer as of the day of the transfer, unless the employee refuses such transfer. If the employee refuses the transfer, the employment relationship ends on the expiry of the statutory notice period; until then, the acquirer and the employee are obliged to perform the contract. The former employer and the acquirer are jointly and severally liable for any claims of an employee which fell due prior to the transfer or which fall due between that juncture and the date on which the employment relationship could normally be terminated or is terminated following refusal of the transfer.

Court practice and academic doctrine define a business as a permanent self-contained organisational unit that is economically autonomous, while a part of a business is an organisational unit that has no such financial autonomy. The provisions of the Swiss Code of Obligations on employee transfers discussed above apply to the transfer of a business (or part thereof) if the transferred business retains the essential features of its identity and the acquirer continues the same or a similar business activity.

5.2 Trade Union or Workers Council Consultation

Where an employer transfers a business, or a part thereof, to a third party (as part of an outsourcing project), he or she must inform the union that represents the employees or, where there is none, the employees themselves reasonably in advance of the contemplated transfer. Information must be given, particularly regarding the reason for the transfer as well as its legal, economic and social consequences for the employees. Where measures affecting the employees are envisaged as a result of such transfer, the union that represents the employees or, where there is none, the employees themselves must be consulted in good time before the relevant decisions are taken.

5.3 Market Practice on Employee Transfers

Parties to an outsourcing arrangement usually carefully consider whether the outsourcing will trigger the transfer of a business, or part thereof, under the Swiss Code of Obligations,

as such transfer would trigger the need to implement the abovementioned measures. By contrast, if the design of the contemplated outsourcing model suggests that there will be no transfer of (a part of) a business, the aforementioned rules will not apply.

As a matter of fact, many outsourcing projects do not fall within the ambit of the provisions of the Swiss Code of Obligations on the transfer of a business, as the conditions summarised above are not fulfilled.

6. Asset Transfer

6.1 Asset Transfer Terms

Movable property

If the outsourcing agreement provides for the transfer of movable property owned by the customer, such as computer hardware, title will pass on the transfer of the relevant asset.

IP rights

If IP rights owned by the customer are to be transferred to the provider, a written agreement will be required, which will typically be contained in the outsourcing agreement. Additionally, change of registration may be required, such as in case of a transfer of trade marks.

Real property

In the unlikely event that the outsourcing project provides for the transfer of ownership in real property, the transfer will require a public deed and registration of the transfer in the real estate register.

Contracts/licences

Where the customer is to transfer contractual rights, such as rights under licence contracts, to the provider, approval must, in principle, be sought from the licensor, except where the licence is not personal or where the customer has already been granted the right to assign the licence to another party. Approval from the licensor may also be required where the parties do not want to transfer the licence, but where the licence agreement provides that using the licensed product (eg, software) in an outsourcing environment requires the licensor's approval. Parties to a contemplated outsourcing arrangement are therefore well advised to conduct careful due diligence on all relevant contracts that may be affected by the outsourcing.

Niederer Kraft Frey Ltd

Bahnhofstrasse 53
CH-8001 Zurich

NIEDERER KRAFT FREY

Tel: +41 58 800 8377
Fax: +41 58 800 8080
Email: andras.gurovits@nkf.ch
Web: www.nkf.ch