Chambers

GLOBAL PRACTICE GUIDES

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

Outsourcing

Switzerland

Law and Practice
and
Trends and Developments

Michael Isler, Jürg Schneider
and Hugh Reeves
Walder Wyss Ltd

chambers.com

2020

SWITZERLAND

Law and Practice

Contributed by:
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss Ltd see p.11

Contents

1. Outsourcing Market

1.1 IT Outsourcing

At a high level, rapid technological advances are impacting IT and BP outsourcing activities. Indeed, behind buzz-words such as "digital transformation", "machine-learning", "AI", "IoT", "cloud computing", "big data" or even "blockchain technology", one finds a new generation of IT tools that have been changing the outsourcing strategies of the market actors. A case in point is the generation of algorithms tailored through machine learning processes. This results in an automation of certain processes which, therefore, provide for the streamlining and speeding up of business activities, mitigation of risks due to human error and generally remain competitive in a continuously evolving environment.

The above, however, does not always mean that businesses are encouraged to outsource more functions than before. On the one hand, many outsourcing providers do indeed have a broad offering of outsourced services, theoretically allowing businesses to focus more than ever before on their core activities. On the other hand, many businesses feel that digital transformation and the internal on-boarding of next generation technologies is necessary to remain relevant in a 21st century market and, thus, choose to retain or even insource certain IT or BP functions.

This has implications in highly regulated sectors such as the financial sector. In this area, the Swiss Bankers Associations published, in March 2019, so-called "Cloud Guidelines" which cover best practices and recommended approaches for "cloud banking". These guidelines, which are not legally binding but should, in effect, be implemented by actors of the Swiss banking industry, have repercussions on outsourcing activities. Indeed, these guidelines call for the outsourcing agreement to cover various aspects such as governance, data processing and audit rights.

Data Protection

Another trend which affects all areas of outsourcing is the area of data protection. On a worldwide level, new data protection laws have been or will be implemented. The EU GDPR is an obvious example, and Switzerland is wrapping up its own legal overhaul as well. These new rules have two primary effects: firstly, they are often much more stringent than the prior generation of rules, thus requiring any entity processing personal data to set up or update its internal practice on the processing of personal data; secondly, there has been a massive increase in public awareness around the issue of data protection and, more specifically, of cybersecurity and data breaches.

These two effects combined have resulted in the spotlight shining directly onto companies who are, therefore, well advised to ensure they have state-of-the-art data security measures in place (either in-house or via their outsourced services provider) and to refresh these on a very regular basis. Again, this encourages some companies to broadly outsource IT activities to specialised providers, while others prefer to keep everything under one roof and become averse to IT outsourcing as a consequence.

COVID-19

The consequences of the COVID-19 pandemic have not been immediately noticeable from an outsourcing standpoint. That said, most companies have incorporated services allowing for remote work and co-operation (eg, Zoom, Google Meets, etc) and this may be interpreted as an indication of more changes to come. Indeed, it is expected that many market actors will seriously consider various outsourcing scenarios in the months or years to come as a palliative measure to make up for the economic consequences of COVID-19 lockdowns and disruptions.

1.2 BP Outsourcing

See **1.1 IT Outsourcing** for general background information on the current outsourcing landscape in Switzerland.

More specifically, regarding BP outsourcing, there has been a marked trend towards shorter-term agreements. There appears to be no single reason for this trend, though the rapid technological change, including "cloudification", plays a role and discourages companies from seeking long-term agreements as it may lock them into a service that may soon lose its relevance. The above-mentioned tension (see **1.1 IT Outsourcing**) between outsourcing and insourcing also reflects the change of approach from some companies concerning their business processes.

1.3 New Technology

For a general overview, see **1.1 IT Outsourcing**.

Technological Innovation

More specifically, the digital transformation experienced with the latest wave of technological innovation has several implications in terms of outsourcing.

Firstly, the providers were generally fast to onboard the latest technologies, in particular cloud services and AI. Despite this early adoption, these technologies have allowed new entrants onto the outsourcing scene and legacy providers are now competing with start-ups and SMEs who often propose novel solutions at a competitive price.

Secondly, many businesses in virtually all areas – from banking and finance, to the industrial field – are loathe to miss out on what is often perceived as a new technological revolution. This leads these companies to bolster their in-house teams and

develop or retain skill-sets even in functions sometimes quite remote from their core competencies. At the very least, businesses must consider how to avoid lock-in effects by allowing proprietary big data learnings to be ring-fenced within service providers without any obligation to have such knowledge transferred back to the customer or passed-on to a successor provider upon termination of the outsourcing agreement.

Finally, it is required to secure a certain level of transparency, thus enabling users to understand the logic behind automated decision making and other self-learning applications.

Blockchain

The distributed ledger technology (frequently referred to as "blockchain"), often coupled with the use of smart contracts, has received a lot of attention in the past years. Rather than being a selling point for providers in a direct outsourcing scenario, parties occasionally use blockchains in joint venture contexts and initially for trial periods or backend functions. It can be noted that the regulatory landscape around certain blockchain-related matters – especially cryptocurrencies and tokens, but also data protection – is still evolving, especially in a transnational context.

Drawbacks

The promises of new technology also come with certain drawbacks. As more and more databases are created and stored, in sometimes remote locations, there has been an increased risk of breaches or loss of data. As mentioned above (see **1.1 IT Outsourcing**), concerns around data security and the resilience of IT systems has taken a central role and become an integral part of the quality assessment when choosing an outsourcing provider. Further, users may want to harvest the expertise and the benefits of new technology by granting service providers greater flexibility in the setup and architecture of their solutions, but without losing control. This is often a difficult balancing act.

1.4 Other Key Market Trends

The pre-existing shift towards cloud solutions will probably intensify in Switzerland. This can be, in part, attributed to the banking and insurance sector where recent regulations and guidelines have brought comfort and certainty to the market and, as a result, incentivised banks and insurances to outsource various functions which otherwise might have remained internalised or partly-outsourced on a local Swiss level so as to avoid cross-border transfers of personal data. The quality of many cloud service offerings also facilitates this trend and additionally offers customers reassurance from a technical perspective as well.

As mentioned above (see **1.2 BP Outsourcing**), there is a trend towards shorter contract durations or, at the very least, more permissive change requests procedures and stricter implementation of pay-per-use models. This trend should last as long as the technological developments progress at the current rate, as it is otherwise hard for the actors to have much predictability on the resilience and quality of the service. Moreover, alternative remuneration models are also on the rise.

COVID-19 has, so far, had only a mild impact on outsourcing activities, though businesses have swiftly adapted their practices from an IT perspective (see **1.1 IT Outsourcing**).

2. Regulatory and Legal Environment

2.1 Legal and Regulatory Restrictions on Outsourcing

Swiss law does not have an over-arching legislation which expressly addresses outsourcing, though various sectorial provisions or regulations do contain rules pertaining to outsourcing. This is, most importantly, the case in the banking and insurance sector with the Swiss Financial Market Supervisory Authority (FINMA) Circular 2018/3 on Outsourcing – banks and Insurers, the so-called "Outsourcing Circular". For further information on this topic, see **2.2 Industry-Specific Restrictions**.

Moreover, as a consequence of data protection legislation, outsourcing activities must typically implement appropriate contractual safeguards as well as proper data security practices. Therefore, these requirements impact outsourcing services. The same applies in specific sectors in which the topical legislation provides for express rules on secrecy; this is, for example, the case in the banking sector, where banking secrecy also may bring about specific requirements related to outsourcing, in particular in a cross-border context.

2.2 Industry-Specific Restrictions

Financial Sector

As outlined in **2.1 Legal and Regulatory Restrictions on Outsourcing**, the financial sector, being strongly regulated and under the FINMA's prudential supervision, has some specific rules on banks and insurance providers outsourcing tasks to third parties. These rules are contained primarily in the Outsourcing Circular.

Moreover, the Swiss Federal Banking Act contains a professional secrecy obligation. Though the Swiss banking secrecy has been subject to international scrutiny and political debate over the past decade, it still plays an important practical role and is a key consideration in the banks' outsourcing strategy. Traditionally, it was often argued that the banking secrecy prohibits banks from transferring abroad any client identifying data (CID) without the client's consent. In reality, the current legal landscape

permits such transfers abroad to a service provider processing said data on behalf of the bank as an auxiliary, provided the necessary safeguards are in place. In this context, the notion of transfer also encompasses hosting abroad of the CID or remote accessing – from abroad – of the CID. Therefore, even if the banking secrecy does not prohibit cross-border transfers of CID, the parties need to carefully assess certain outsourcing activities (eg, hosting abroad).

Proper outsourcing conduct

The Outsourcing Circular in its current form entered into force on 1 April 2018. The purpose of this circular, which applies to banks, securities dealers and insurance providers, is not per se to limit outsourcing but rather to circumscribe it and set out a proper conduct. It does so by following a principles-based and technology-neutral approach. In particular, the Outsourcing Circular calls for a regularly updated inventory of outsourced functions, proper selection, instruction and monitoring of the outsourcing service provider, as well as audit and supervision considerations. In practice, the requirements of the Outsourcing Circular materialise in a written outsourcing agreement which must meet the standards set out in the Outsourcing Circular.

The Outsourcing Circular can be seen as imposing restrictions on outsourcing in the financial sector. It does indeed prohibit the outsourcing of key functions such as direction, central executive management and strategic decision-making functions. Nevertheless, since its entry into force (1 April 2018), it has played more of a facilitating role rather than bringing about additional administrative hurdles. The targeted actors appear to have been receptive to this new version of the Outsourcing Circular and generally agree that it has, if anything, increased the appeal of foreign providers by offering pragmatic and workable solutions.

Furthermore, the Outsourcing Circular does not subject outsourcing activities to a specific authorisation. However, as regards the insurance sector and based on insurance surveillance legislation, the insurance companies must communicate to FINMA, before-hand, any contemplated outsourcing which includes the delegation of important function to the outsourcing provider. Unless FINMA opens an examination procedure within four weeks upon receipt of said communication, FINMA approval is deemed given.

Operational risks for banks

Another FINMA circular, 2008/21 on the operational risks for banks (Circular 2008/21) sets out various rules on data security and breach notification, as will be further detailed hereunder (see **2.3 Legal or Regulatory Restrictions on Data Processing or Data Security**).

FINMA revised (entry into force on 1 January 2020) the Outsourcing Circular and the Circular 2008/21, among others, as a result of legal and regulatory changes affecting small-sized banks. Indeed, the industry generally considers the regulatory and administrative requirements on small financial institutions in Switzerland overly complex and burdensome. The revised circulars did bring some administrative relief to small-sized banks and also allow the outsourcing parties to bypass an approval obligation (that existed previously) concerning subcontractors. Parties nonetheless remain free to include a prior approval requirement in their outsourcing contracts should they so desire.

Telecommunications Sector

Companies active in the telecommunications sector may look to outsource various facets of their activities. In this respect, the TCA enshrines the so-called "telecommunications secrecy". This is an obligation upon anyone who provides a telecommunications service, and this notion is currently broadly interpreted. That being said, it can be argued that if an outsourcing provider exclusively processes the data covered by the telecommunication secrecy on behalf of the telecommunication service provider in order to allow the telecommunications services provider to render its services and invoice its customers, no specific additional consent is required by the telecommunication service provider's customers. In any case, as for the financial sector, it is important that the telecommunication services provider carefully assesses the situation prior to entering into an outsourcing agreement and takes the necessary measures.

In this area, the growing trend around IoT devices is expected to lead to increasing exposure under the TCA as the information pertaining to one single customer may be shared between various providers of IoT devices and telecommunications services. This exposure is increased by the above-mentioned broad interpretation given to the notion of telecommunications services. In turn, outsourcing deals may, unbeknownst to the parties, include telecommunications-related aspects.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

General Considerations on Data Protection and Data Security

Switzerland's data protection legislation is primarily contained in the Federal Data Protection Act (FDPA) of 19 June 1992, as well as its implementing ordinance (FDPO). Historically, Switzerland has offered a strong level of data protection and its legislation, being technology-neutral, has proven resilient over the years. Nevertheless, with the revamping of the EU's data protection legislation, and due to Switzerland's international commitments, a total overhaul of the FDPA began in 2016 and the final draft of the revised FDPA was adopted by the parliament

on 25 September 2020. Entry into force of the revised FDPA should occur in the course of 2022, though there is currently no confirmed date. Of note is the general alignment (though not a full match) with the requirements under the GDPR; therefore, cross-border data flows between Switzerland and EU/EEA jurisdictions will generally remain unhindered. Moreover, but only as a rule of thumb, an outsourcing set-up that complies will the GDPR will, overall, be in line with Swiss data protection legislation, though the parties will have to perform a case-by-case analysis given the criticality of this area and include any Swiss specifics in the contractual documentation.

Data security remains an important topic for any companies engaging in outsourcing as data breaches are now a major risk for virtually any business. Swiss data protection legislation does not define strict standards for data security. Rather, it calls for companies to ensure they follow state-of-the-art industry best-practice to prevent unauthorised processing of personal data. This is in reference to the various relevant technical standards, such as the ISO27000 family of security standards. The Swiss legislator again avoided providing a list of technical requirements, preferring to rely on its technology-neutral stance, thereby allowing the data protection legislation to remain relevant despite fast technological change. In this respect, Switzerland does not have any data territoriality requirements under its data protection legislation and, hence, there is no obligation to store and/or otherwise process personal data in Switzerland (limitations and/or special requirements may however result from sector specific legislations).

General Permissibility of Cross-Border Transfers; the "Outsourcing Privilege"
The FDPA sets certain requirements in cases where an entity entrusts third parties acting as processors in the context of an outsourcing. A customer may, therefore, entrust data processing activities to an outsourcing services provider as processor if certain conditions are met. In this case, no consent is required under the FDPA. This allows the outsourcing to take place seamlessly and is frequently referred to as the "outsourcing privilege". Please note that, unlike the GDPR, the FDPA does not require a minimum set of topics to be covered by the outsourcing contract.

In the financial sector (as well as in other sectors), additional requirements may apply to the contractual relationship and its implementation.

Finally, it must be noted that so-called "blocking statutes" must be considered in case of outsourcings to foreign entities. It can in our view be argued that if an outsourcing provider acts as an auxiliary of the customer, and provided that the auxiliary exclusively uses the information provided by the customer on behalf of such customer, that the blocking statutes do not as such prohibit an outsourcing.

Safeguards
A key consideration in any outsourcing is the implementation of the proper safeguards in cross-border transfers of personal data.

In cases where personal data is transferred to outsourcing providers located in countries that the Swiss Federal Data Protection and Information Commissioner (FDPIC) deems to offer an equivalent level of data protection for the personal data concerned, no specific additional safeguards are required. If transfers are to countries that do not qualify as offering an equivalent level of data protection for the personal data being transferred – including the United States after the de facto fall of the Swiss-US Privacy Shield in September 2020 – the parties need additional safeguards. These are typically contractual safeguards based on the EU model clauses (named Standard Contractual Clauses (SCC)) adapted to Swiss law requirements.

However, according to the FDPIC and in line with the European Court of Justice's reasoning in the "Schrems II" case, the SCCs fail in many cases to provide an adequate level of data protection. Thus, Swiss data exporters are required to check by means of a case-by-case risk assessment if their current outsourcing practice needs to be adapted. In particular, Swiss-based companies should assess the practical risk of a data access by foreign authorities. Where the risk analysis reveals that the standard clauses are insufficient, contractual amendments and/or, where feasible, technical means such as encryption and/or pseudonymisation need to be implemented to prevent such access. If neither contractual amendments nor technical measures can adequately counteract the risks, changing the service location to a country with an adequate level of data protection should be considered.

Further, as a matter of standard practice and irrespective of the applicability of the GDPR, parties generally enter into data processing agreements (or addenda, depending on the terminology of choice) which now live up to the requirements of the GDPR, though adapted to Swiss legal requirements, when an outsourced services provider processes personal data on behalf of its client.

2.4 Penalties for Breach of Such Laws
A breach of the Swiss data protection legislation may give rise to a criminal law fine of up to CHF10,000. The revised (but not yet in force) Swiss data protection legislation foresees that the criminal law fines will be increased to an amount of CHF250,000 and applied to a broader scope of offenses.

As a side note, a breach of the Swiss banking secrecy can lead to a five-year prison sentence if there is an enrichment intent, three years in other intentional cases, or, in case of negligence, to a fine of up to CHF250,000. In addition, a violation of the telecommunications secrecy may give rise to a three-year prison sentence or a fine.

2.5 Contractual Protections on Data and Security

Swiss practice often followed a rather "hands-off" approach in this respect. Nowadays, in general, parties agree on detailed technical measures, especially in the case of sophisticated customers, in high-stakes contracts or sensitive data being concerned. Therefore, the language currently relating to technical measures is extensive, detailed and leaves little room for interpretation. Moreover, the increased attention given to data protection compliance has encouraged businesses to set out clear data protection and data security rules, list the standards (for instance, the ISO27000 family of standards), and provide for in-depth audit rights. For reasons of (insufficient) experience and know-how, many smaller companies do, however, still struggle with the above, with the consequence that it is often difficult to determine whether or not the actual technical measures in place are sufficient for the client's needs and risk exposure.

3. Contract Models

3.1 Standard Supplier Customer Model

The standard supplier customer model in Switzerland remains the master agreement model, as the case may be, completed by local agreements. In this configuration, the parties enter into a framework agreement and a set of exhibits. The latter defines the scope, service levels, performance measurement scheme, financial considerations and so forth.

This model has proven effective and remains popular given its broad use and the market's rich experience with it.

3.2 Alternative Contract Models

Multi-sourcing

Multi-sourcing is common, both in IT and BP outsourcings. Clients enjoy the choice of providers and frequently choose a multi-sourcing approach, as this not only allows them to tailor the outsourcing to their needs but may also serve to reduce costs. In terms of costs, a variety of payment options have come on the market in recent years, such as "pay-as-you-go" billing, which is often more appealing in comparison to the more traditional unit price model. Multi-sourcing may, however, result in more complexity as a greater number of parties are involved, thus requiring excellent corporate governance and proper management processes.

The service integration and management (SIAM) approach, which has become fairly popular in some jurisdictions, has not yet matured in Switzerland, but clients are increasingly convinced that it may be worthwhile to entrust service providers with at least part of the co-ordination tasks. Further, multi-sourcing entails the need of introducing a "fix first, settle later" rule in order to avoid finger-pointing between various service providers, ideally enriched with a mechanism governing the financial compensation in case providers are compelled to act outside their sphere of responsibility.

Joint Ventures

Joint ventures are sometimes used for outsourcing purposes. In this scenario, the outsourcing party (client) will look to retain strong oversight, or even control, over the outsourced service, while the service provider will allocate resources to the joint venture and ensure its proper functioning. Joint ventures make the most sense when the client already has know-how and expertise in the outsourced service and is seeking to retain and further develop said know-how and expertise. Therefore, joint venture situations are particularly useful when they involve the use (or development) of next generation technologies.

They are also a good fit when the outsourcing services provider will need to rely on some technology owned by its client, as the joint venture model allows to properly protect ownership, use and future developments of the technology. Another popular use case for joint ventures are shared utilities, which are often developed in the realm of emerging technologies such as distributed ledger technology. The purpose of these joint ventures is not to retain a certain level of know-how partially in-house, but rather to enable the pooling of forces among industry peers to create an ecosystem with sufficient scalability.

3.3 Captives and Shared Services Centres

There does not appear to be a clear and strong trend in relation to captives and shared services centres. Resorting to captives and service centres may appear a valid option to companies looking to insource processes, while at the same time benefitting from the cost-saving advantages of remote centres outside of Switzerland. That said, the other outsourcing mechanisms mentioned above (**3.2 Alternative Contract Models**) should remain prevalent and it is not expected that captives and shared services centres will grow in popularity in the near future.

4. Contract Terms

4.1 Customer Protections

Contractual warranties and liability provisions are ubiquitous in outsourcing agreements. These serve to reassure the customer that the outsourcing services provider will perform its

tasks with proper care, skilled personal, in compliance with all applicable legal requirements, and so forth. Through liabilities, the customer may try to shift onto the contracting party the financial consequences of certain damaging events (infringement of third-party intellectual property, for instance). Warranties and liabilities are, however, only one type of incentive on the outsourcing services provider to actually perform the agreed-upon services.

A proper definition of the scope of the services is of the utmost importance in outsourcing agreements and is a key factor in customer satisfaction. This definition of the scope must be accompanied by proper measurement tools. In order to ensure that the key performance indicators (KPIs) and service levels are met, the parties should define adequate measurement methods, for instance by using the "SMART" metric: Specific Measurable Relevant and Time-based.

In terms of timely service delivery, realistic KPIs and milestones are also necessary. Customers often look to combine said KPIs or milestones with a bonus or malus system (eg, contractual penalties, which are generally lawful in Switzerland), as this is an effective way of ensuring proper performance. In cases where the customer considers it is not receiving satisfactory services, it may also want to resort to step-in rights, whereby the customer or a third party intervenes in the provision of the services.

Parties often focus on change requests, as these may have a substantial impact on the pricing. From a customer-protection stand-point, change requests can indeed be a double-edged sword and customers are well-advised to advocate in favour of a precise and predictable change request process. The same can be said of the governance provisions, whereby the parties should aim for a smooth and responsive interaction in governance-related aspects.

In longer-term agreements, benchmarking gives both parties a helpful reference point and allows the customer to compare the services it is receiving with those of other potential providers.

4.2 Termination

Swiss law gives the parties broad leeway when it comes to contractual provisions. This so-called "contractual freedom" is especially strong in business-to-business relationships. Hence, parties can provide for various termination modalities, be it termination for convenience or termination for cause.

Market practice is to rely on a fixed term, with one or two extension options available to the customer at the end of the fixed terms. In these situations, termination for convenience prior to the initial fixed terms by the customer usually would come with a so-called "exit fee", ie, an amount to be paid by the customer in case of termination for convenience. Suppliers will not have any right to termination for convenience prior to the fixed term (or the aforementioned extension periods).

Termination for cause addresses pre-defined situations where a contractual breach by the other party or any other pre-defined event will entitle a party to terminate the outsourcing agreement. These situations may be diverse, such as an outsourcing service provider's under-performance, a party's breach of its duty of confidentiality, the customer's repeated late payment, change of control, non-alignment of pricing post-benchmarking and so forth. It is also possible to provide for a termination for cause in more generic terms, such as "in case of a material breach of the outsourcing agreement". Though this wording is also common, it is somewhat risky given the complexity of outsourcing agreements and the varying interpretations of what could constitute a "material breach". This being said, customers in practice strive to limit the valid causes entitling service providers to terminate the contract to qualified payment defaults.

Generally, the parties to an outsourcing agreement also address, in detail, the consequences of the termination. Indeed, when these provisions are absent, business continuity pertaining to the outsourced service is at risk and the customer must ensure a seamless provision of the services. On the other hand, the outsourcing services provider will look to charge wind-down fees to cover the costs involved in this post-termination phase.

4.3 Liability

Swiss law does, in various cases, distinguish between direct and indirect damages or losses. Typically, Swiss law, as well as the Swiss courts, looks at causation to determine whether a loss the parties – or a judge – can attribute to an initial damaging event or if causation is too weak to do so. In other words, any loss that appears as a consequence (whether direct or indirect) of one specific damaging event can qualify as a recoverable loss. Nevertheless, given the contractual freedom (see **4.2 Termination**), the parties are free to define damaging events as they wish, including damages suffered by affiliates and service recipients. In that respect, it remains advisable as a matter of predictability, to define the categories of losses which the parties wish to include or exclude (for instance, loss of profits, etc).

In any case, whether discussing matters of direct or indirect loss, Swiss law does not allow an exclusion in advance of liability in cases of gross negligence or wilful misconduct of a party. That means that provisions implementing a monetary cap to one party's liability will not apply if that party acted in gross negligence or with intent.

Loss of profit is frequently addressed in contracts. However, loss of goodwill, business or even the loss of an opportunity are not systematically discussed in outsourcing agreements.

The parties may often discuss other types of losses. For instance, loss of data and costs for restoring lost data also constitutes an oft-negotiated item given the data's central role in outsourcing agreements.

4.4 Implied Terms

The notion of implied terms is somewhat alien to Swiss law. Indeed, where the contract does not provide for a term, Swiss law – namely the Swiss Code of Obligations (SCO) – will apply. Therefore, if a contract is quiet on a specific question, the judge will automatically look to the SCO to fill that gap.

This allows the parties to streamline many parts of any given agreement. However, the SCO does not govern the outsourcing agreement as such. Instead, the outsourcing agreement is a patchwork of various agreements under the SCO. More specifically, the outsourcing agreement usually combines properties of the work contract, lease contract, purchase contract and even a mandate. This mixed legal nature in turn encourages the parties to clearly express all key elements of their understanding in a dedicated outsourcing agreement, thereby mitigating risks of adverse or simply unexpected court interpretations should a dispute arise.

5. HR

5.1 Rules Governing Employee Transfers

Swiss law has rules governing employee transfers, which may apply in outsourcings. In an outsourcing environment, these rules are colloquially referred to by their British denomination of TUPE (Transfer of Undertakings Protection of Employment) regulations.

The SCO provides that when a business or part thereof is transferred, so are the employees, unless they refuse. In case of employee refusal, their employment contract ends upon expiry of the notice period.

The rules on employee transfers often do not apply to outsourcings as the outsourced service often does not qualify as a business or part thereof. Because of the important consequences of employee transfer rules, the parties always need to consider this aspect carefully prior to executing an outsourcing agreement.

5.2 Trade Union or Workers Council Consultation

If TUPE requirements apply, the employer must provide transparent information concerning the purpose of the transfer and its implications to the trade union, if any, or the employees themselves. If the outsourcing impacts the employees, a consultation must take place in due course and prior to the outsourcing process moving forward.

5.3 Market Practice on Employee Transfers

As mentioned above (see **5.1 Rules Governing Employee Transfers**), outsourcings often do not trigger TUPE regulations. Nevertheless, should they do so, the parties must comply strictly with the respective legal requirements. There is, therefore, little room for any diverging market practice. However, the parties will, in general, contractually address the financial costs (should employees transfer to the service provider and vice-versa at the end of the outsourcing), as well as co-operation and information duties.

Parties experienced in outsourcing – as providers or as customers – will know that TUPE regulations are part of the pre-contractual assessment and will act accordingly by analysing the situation to determine whether or not the contemplated outsourcing will give rise to TUPE regulation requirements.

6. Asset Transfer

6.1 Asset Transfer Terms

At a high level, parties can generally easily transfer assets under Swiss law. The nature of the asset at stake however determines the legal modalities and formalities of the transfer.

The underlying contracts necessary for the performance of the outsourcing may be assigned depending on the provisions of the underlying contract (which might provide for an express prior consent of the counterparty), or through a simple assignment form. This applies for instance to the transfer of license agreements over software, contracts with various pre-existing third-party providers (eg, IT server space provider), and so forth. If the underlying contract requires consent for the assignment, such consent should be sought. Should it not be obtained, for timing and practical reasons, work-around must be implemented.

The parties will transfer IP rights in a written agreement. The assigning party will typically agree to update any public IP register accordingly, thereby allowing the assignment to deploy third-party publicity effect.

The transfer of real estate requires a notarised deed, though the transfer of chattel is not subject to a specific form (written form is recommended).

In any case, irrespective of the nature of the assets, the agreement transferring said assets must address the expected or promised qualities of those assets. It should do so through representations and warranties may be more or less extensive depending on the negotiations and the parties' requirements and experience.

Walder Wyss Ltd is a dynamic presence in the market and one of the most successful Swiss commercial law firms. The firm specialises in corporate and commercial law, banking and finance, intellectual property and competition law, dispute resolution and tax law. With around 220 legal experts from offices in Zurich, Geneva, Basel, Berne, Lausanne and Lugano, the firm provides clients with a seamless one-stop shop, and personalised and high-quality services in all language regions of Switzerland. Clients include national and international companies, publicly held corporations and family businesses as well as public law institutions and private clients.

Authors

Michael Isler is a partner in the intellectual property, information technology and data protection product groups. He regularly advises in complex outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. He further enjoys a vast experience in copyright, trade mark and patent law. A particular focus of his work is the life sciences and health sector. Michael regularly publishes and lectures in his practice areas and takes an active role in several professional organisations. He is co-editor of a Swiss law journal for pharma, biotech and medtech.

Hugh Reeves is a senior associate in the intellectual property, information technology and data protection product groups. His preferred areas of practice include technology transfers, copyright, patent, trade mark and trade secret law as well as information technology law. Hugh is also active in the areas of data protection and privacy laws.

Jürg Schneider is a partner at Walder Wyss and head of the Lausanne office. His practice areas include information technology, data protection, and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration, and global outsourcing projects. Jürg has deep and extensive experience in the fields of data protection, information security, and e-commerce, with a particular focus on transborder and international contexts. In addition, he regularly publishes and lectures on ICT topics and is a member of several professional organisations. He is a member of the board of directors of the International Technology Law Association and former co-chair of its data protection committee.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss

Trends and Developments

Contributed by:
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss Ltd see p.14

Accurately identifying trends in the Swiss outsourcing field is a delicate exercise. Undeniably, there have been certain sustained market practices that have proved consistent over the years and will remain relevant in the years to come. However, a combination of factors – some predictable and others the result of pure happenstance – have brought about uncertainty and confusion.

Indeed, the COVID-19 pandemic has wreaked havoc on national and international markets, led to countless job and financial losses and caused companies big and small to reassess their practices. This all comes against a backdrop of important regulatory changes, in Switzerland and abroad, and growing suspicions linked to certain technologies or their providers.

"Digital Transformation"
Until early 2020, the biggest impact on the outsourcing industry came from new technologies, in particular relating to cloud computing and artificial intelligence (AI) and big data. Other technologies or business practices had also been enjoying a growing disruptive factor as was the case with the blockchain, also called distributed ledger technology (DLT), and the "internet of things" (IoT). This technological landscape allowed, or even required, many businesses to digitalise many of their practices in a process often referred to as the "digital transformation".

This process does not necessarily involve any actual outsourcing as companies may implement these changes internally, for instance by onboarding a new cloud service on a software as a service (SaaS) delivery model. It does, however, bear a striking resemblance to outsourcing in its result as it allows the customer to streamline its business, optimize its resource allocation and generally increase efficiency. Moreover, the contracting set-up is in some ways comparable to a conventional outsourcing structure, typically involving a master services agreement and schedules with various key performance indicators (KPIs), technical and data security requirements and so forth.

A noteworthy differentiator of these contracts is their very high degree of standardisation and their relatively short minimum term. Indeed, customers usually look to avoid any lock-in effect with a single provider and rather preserve their option to move to another provider, for instance in case of a new and more advantageous rival technology. Conversely, on the provider side, the approach often appears to be geared around the avoidance of customer termination, usually through automatic contract renewal, few business continuity commitments in case of termination, long termination notice periods, and so forth.

These above trends do remain relevant at the time of writing and are expected to gain further traction as companies look to remain at the forefront of technological evolution, either out of fear of missing out, commercial considerations or simply from a pure marketing perspective. In this respect, though the old trend of outsourcing as a way for companies to focus solely on their core competencies still remains absolutely true and relevant, the counter-current, ie, retaining or insourcing secondary competencies or functions, applies as well and is expected to gain traction.

COVID-19 and 5G Technology Providers
Presently, the COVID-19 pandemic as well as various disputes around the safety or reliability of certain offshore providers has led most all businesses to question their approach to outsourcing or on-boarding third-party technologies.

Firstly, because of the COVID-19 pandemic and its economic fallout, many Swiss companies have been forced to rethink their business models and, frequently, look at ways to further reduce their overhead and operating expenses. Given the above-mentioned tension between, on the one hand, the historical benefits of outsourcing to providers based abroad in order to retain only pre-defined core competencies and, on the other hand, the perceived added value in achieving a holistic digital transformation that would on-board certain new technologies and services rather than reallocate them to a third party, the current situation is a cause for concern for many businesses. Indeed, it means that they have to deal with a high amount of uncertainty and do not have a clear roadmap going forward. At the time of writing, it is hard to extract any clear trend and no consistent momentum has yet emerged.

Secondly, there has been discussion and questions around the reliance on certain IT services providers. A much-discussed example over the past year has been a multinational Asian 5G technology provider that has come under scrutiny in North America and Europe for its alleged ties with the government. Because this multinational company is an important player in the field of 5G essential technologies, which constitute critical infrastructures as national means of communications would rely on them, many governments have had to take a stance on the admissibility of this provider in the 5G context. The Swiss

government has not imposed any limitation on the reliance on any of the international service providers or their products and services.

All in all, however, this international scrutiny of an important IT provider has led many companies, of all sizes, to rethink their outsourcing practices as they wish to steer clear of any business association that may result in negative market perception or turn out to be a legal or regulatory liability. In this respect, Swiss companies have appeared rather adept at so-called "nearshoring" (for the sake of this article, "nearshoring" can be defined as outsourcing to a provider located in a neighbouring country or a close country from a geographical and cultural perspective). This is reinforced by the stringent data protection requirements applicable inter alia to Swiss-based companies as well as certain sectoral rules and guidelines (eg, in the banking sector), which often leads Swiss companies to remain cautious when outsourcing to or acquiring services from providers based outside of the EU or, even, outside of Switzerland.

Evolving Legislation

In recent years, Switzerland has been bolstering its rules in several areas central to outsourcing activities.

Telecommunications legislation and, in particular telecommunications surveillance legislation gives broad investigative powers to Swiss criminal prosecution authorities. This may impact tech providers given the comparatively inclusive definition of telecommunications (or similar) services. In other words, outsourced services providers looking to offer their services to Swiss customers frequently have to assess their services also under a Swiss telecommunications regulatory lens.

On 25 September 2020, the Swiss Parliament adopted what should be the final text of the draft revised Federal Data Protection Act (FDPA). This revised FDPA, which should not enter into force before 2022, is generally consistent and in line with the requirements of the European Union's General Data Protection Regulation (GDPR). Though the revised FDPA does not stray far from the (currently in force) FDPA, it will bring about increased legal obligations on data controllers and processors alike and empower the Swiss authorities to levy more significant fines than is the case currently (CHF 250'000 compared to a maximum fine of CHF10,000 in certain – limited – circumstances).

The EU and Switzerland both invalidated (either expressly or, in the case of Switzerland, in effect) the Privacy Shield framework in July, respectively September 2020. This framework, which came in two iterations, namely the Swiss-US and the EU-US Privacy Shield frameworks, greatly facilitated cross-border personal data disclosures from Swiss/EU-based companies to USA-based ones. The fall of the Privacy Shield framework and the related weakening of the so-called "standard contractual clauses" (or SCC) require Swiss-based companies that use service providers based in countries that do not provided for an adequate protection for the personal data processed by such service provider, to check by means of a risk assessment if their current outsourcing practice is still in line with data protection requirements. Depending on the result of such risk assessment, current outsourcing practices may have to be adapted (for example, as the case may be, by contractual changes, by technical means such as encryption and/or pseudonymisation, by changing the service location, etc).

"Local" Outsourced Services

In light of the above considerations, there seems to be several arguments in favour of a more "local" sourcing of outsourced services. This seems to be reflected in the approach of several key players (and outsourcing customers) on the Swiss market who have come to expect more geographic proximity from their contractual partners. This is especially true in the banking and finance sector, being specified that the banking industry and the prudential authority (FINMA) have issued various texts, recommendations, circulars and guidelines that look to facilitate bank outsourcing activities, including to service providers located outside of Switzerland.

Moreover, because the Swiss legal requirements are increasing in complexity, it is becoming increasingly important for customers to ensure that any contemplated outsourced services provider not only offers the services at a viable price point but also meets certain "quality" guarantees (such as for instance compliance with data security and telecommunications surveillance requirements). This has been leading to service providers strengthening their physical presence in Switzerland, thereby mitigating many of their customer's concerns.

Conclusion

In summary, we believe that outsourcing will, in one form or another, play a central role for many service providers active in Switzerland and their Swiss-based customers. Indeed, sustained outsourcing deals are expected. That said, it is also expected for customers to place higher scrutiny on their potential contractual partners given the developments in the Swiss (and international) legal landscape and the uncertainties of doing business in a COVID-crippled world. Therefore, rather than attempt to follow current trends, one may on the contrary look for creative yet carefully analysed approaches to outsourcing, both from the customer and from the service provider perspective.

Walder Wyss Ltd is a dynamic presence in the market and one of the most successful Swiss commercial law firms. The firm specialises in corporate and commercial law, banking and finance, intellectual property and competition law, dispute resolution and tax law. With around 220 legal experts from offices in Zurich, Geneva, Basel, Berne, Lausanne and Lugano, the firm provides clients with a seamless one-stop shop, and personalised and high-quality services in all language regions of Switzerland. Clients include national and international companies, publicly held corporations and family businesses as well as public law institutions and private clients.

Authors

Michael Isler is a partner in the intellectual property, information technology and data protection product groups. He regularly advises in complex outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. He further enjoys a vast experience in copyright, trade mark and patent law. A particular focus of his work is the life sciences and health sector. Michael regularly publishes and lectures in his practice areas and takes an active role in several professional organisations. He is co-editor of a Swiss law journal for pharma, biotech and medtech.

Hugh Reeves is a senior associate in the intellectual property, information technology and data protection product groups. His preferred areas of practice include technology transfers, copyright, patent, trade mark and trade secret law as well as information technology law. Hugh is also active in the areas of data protection and privacy laws.

Jürg Schneider is a partner at Walder Wyss and head of the Lausanne office. His practice areas include information technology, data protection, and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration, and global outsourcing projects. Jürg has deep and extensive experience in the fields of data protection, information security, and e-commerce, with a particular focus on transborder and international contexts. In addition, he regularly publishes and lectures on ICT topics and is a member of several professional organisations. He is a member of the board of directors of the International Technology Law Association and former co-chair of its data protection committee.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss