Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Technology & Outsourcing 2022

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

Switzerland: Law & Practice
and
Switzerland: Trends & Developments

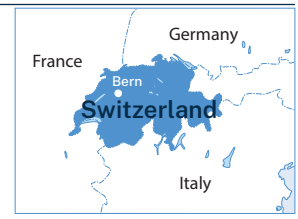
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss Ltd

practiceguides.chambers.com

SWITZERLAND

Law and Practice

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



Contents

1. Market

1.1 IT Outsourcing

At a high level, rapid technological advances are impacting IT and business process (BP) outsourcing activities. Indeed, behind buzzwords such as "digital transformation", "machine learning", "AI", "internet of things (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 helps to streamline and speed up business activities, mitigate against risks due to human error and generally remain competitive in a continuously evolving environment.

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

This has implications in highly regulated sectors such as finance. In the financial sector, the Swiss Bankers Association published its so-called Cloud Guidelines in March 2019, which cover best practices and recommended approaches for "cloud banking". These guidelines, which are not legally binding but should in effect be implemented by those operating in the Swiss banking industry, have repercussions for 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 that 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's General Data Protection Regulation (GDPR) is an obvious example; however, Switzerland has also overhauled its data protection legislation, which is set to enter into force in September 2023.

These new rules have had two primary effects, namely:

- any entity processing personal data must now set up or update its internal practice on the processing of personal data, as this legislation is often more stringent than the previous generation of rules; and
- a massive increase in public awareness around the issue of data protection and, more specifically, of cybersecurity and data breaches.

These two effects have combined to shine the spotlight directly on companies, who would be 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 reassess and update these on a regular basis. This encourages some companies to broadly outsource IT activities to specialised providers, whereas others prefer to keep everything under one roof and – as a consequence – become averse to IT outsourcing.

COVID-19

The effects of the COVID-19 pandemic have not been immediately noticeable from an outsourcing standpoint, although it has prompted most companies to speed up their digitalisation processes. That said, most companies have incorporated services allowing for remote work and co-operation (eg, Zoom, Google Meets) and this may be interpreted as an indication of more changes to come.

Indeed, market actors have been envisaging or implementing various outsourcing scenarios, perhaps as a palliative measure to make up for the economic consequences of COVID-19 lockdowns and disruptions. Although it is too early to outline clear trends, it would appear that Swiss companies are not necessarily outsourcing more but, rather, are outsourcing differently compared to the pre-pandemic period. This could allow new market entrants and bring new technologies to the forefront.

1.2 Business Process Outsourcing (BPO)

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

More specifically, there has been a marked trend towards shorter-term agreements in the case of business process outsourcing (BPO). There appears to be no single reason for this trend; however, 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 tension mentioned in **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

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

First, 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 into 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 technological revolution. This leads 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 necessary to secure a certain level of transparency, thereby enabling users to understand the logic behind automated decision-making and other self-learning applications.

Blockchain

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 back-end 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 in **1.1 IT Outsourcing**, concerns around data security and the resilience of IT systems have taken a central role and become an integral part of the quality assessment when choosing an outsourcing provider. Furthermore, users may want to harvest the expertise and the benefits of new technology by granting service providers greater flexibility in the set-up and architecture of their solutions, but without losing control. This is often a difficult balancing act.

2. Regulatory and Legal Environment

2.1 New Legal and Regulatory Restrictions on Technology Transactions or Outsourcing

Swiss law does not have an over-arching legislation that expressly addresses outsourcing, although various sectorial provisions or regulations do contain rules pertaining to outsourcing. This is most notable in the banking and insurance sector, which has the Swiss Financial Market Supervisory Authority (FINMA) Circular 2018/3 on Outsourcing – Banks and Insurers (the "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 where the topical legislation provides for express rules on secrecy – for example, banking secrecy may also bring about specific requirements related to outsourcing, particularly 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; however, financial sector actors have increasingly taken a more global legal approach to outsourcing and thus also look to comply with the European Banking Authority (EBA)'s guidelines on outsourcing.

Moreover, the Swiss Federal Banking Act contains a professional secrecy obligation. Although Swiss banking secrecy has been subject to international scrutiny and political debate during the past decade, it still plays an important practical role and is a key consideration in the banks' outsourcing strategy.

It was traditionally 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 land-

scape 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 the CID abroad or remotely accessing the CID from abroad. 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. 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 that meets 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, as opposed to bringing about additional administrative hurdles. The targeted actors appear to have received this new version of the Outsourcing Circular well and generally agree that, if anything, it has 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, based on insurance surveillance legislation, companies in the insurance sector must inform FINMA beforehand of any contemplated outsourcing that involves delegating important functions 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, Operational Risks – Banks ("Circular 2008/21"), sets out various rules on data security and breach notification (and is further detailed in **2.3 Legal or Regulatory Restrictions on Data Processing or Data Security**).

FINMA revised the Outsourcing Circular and the Circular 2008/21 (entering into force on 1 January 2020) 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 allowed the outsourcing parties to bypass a previous approval obligation 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 Federal Telecommunications Act (TCA) of 30 April 1997 enshrines so-called telecommunications secrecy.

Telecommunications secrecy is an obligation shared by 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 telecommunications secrecy on behalf of the telecommunications 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 telecommunications service provider's customers. In any case, as per the financial sector, it is important that the telecommunications services provider carefully assesses the situation prior to entering into an outsourcing agreement and takes the necessary measures.

On a related note, the growing trend for IoT devices is expected to lead to increasing exposure under the TCA. This is because 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 owing 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 legislation will occur on 1 September 2023.

Of note is the general alignment (albeit not a full match) with the requirements under the GDPR; hence, cross-border data flows between Switzerland and EU/EEA jurisdictions will generally remain unhindered. Moreover, an outsourcing set-up that complies with the GDPR will be – overall – in line with Swiss data protection legislation, but only as a rule of thumb. However, given the criticality of this area, the parties will have to perform a case-by-case analysis 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. As a result, 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 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 is important to note that so-called blocking statutes must be considered in the case of outsourcings to foreign entities. It can be argued that the blocking statutes do not prohibit an outsourcing 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.

Safeguards

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

No specific additional safeguards are required in cases where personal data is transferred to outsourcing providers located in countries that are deemed by the Swiss Federal Data Protection and Information Commissioner (FDPIC) to offer an equivalent level of data protection for the personal data concerned. 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 USA after the de facto fall of the Swiss-US Privacy Shield in September 2020), the parties need additional safeguards. These are typically contractual safeguards that are based on the EU model clauses known as Standard Contractual Clauses (SCC) but 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 original SCCs failed on many fronts to provide an adequate level of data protection. In September 2021, the FDPIC recognised the new SCCs adopted by the EC on 4 June 2021, provided that the necessary adaptations and amendments to such new SCCs are made for use under Swiss data protection law. Accordingly, the FDPIC called for their use from 27 September 2021 onwards (with a transitory period expiring on 1 January 2023 in case the "old" SCCs were already in place).

Swiss-based companies should systematically assess the practical risk of a data access by for-

eign authorities in addition to their cross-border data transfer practices. Where the risk analysis reveals that the SCCs are insufficient, contractual amendments and/or 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.

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) that now live up to the requirements of the GDPR – albeit adapted to Swiss legal requirements – when an outsourced services provider processes personal data on behalf of its client.

3. Contract Models

3.1 Standard Supplier Customer Model for Outsourcing

The standard supplier customer model in Switzerland remains the master agreement model, albeit completed by local agreements where appropriate. 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 for Outsourcing

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. One example is "pay-as-you-go" billing, which is often more appealing when compared with the more traditional unit price model. Multi-sourcing may result in more complexity, however. A greater number of parties are involved; therefore, excellent corporate governance and proper management processes are required.

The service integration and management (SIAM) approach, which has become fairly popular in some jurisdictions, has not yet matured in Switzerland. Clients are nonetheless increasingly convinced that it may be worthwhile to entrust service providers with at least part of the coordination tasks.

Multi-sourcing also entails the need to introduce a "fix first, settle later" rule in order to avoid finger-pointing between various service providers. Ideally, this would be enriched by 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 func-

tioning. 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 (eg, 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 Digital Transformation

This issue is not relevant in Switzerland.

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 personnel, 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 for 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 example, by using the “SMART” (Specific, Measurable, Relevant and Time-based) metric.

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 believes 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 standpoint, 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 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 – that is, 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. The range of these situations is 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". Although 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". Having said this, in practice customers strive to limit the valid reasons for terminating the contract to qualified payment defaults.

Generally, the parties to an outsourcing agreement also address the consequences of the termination in detail. 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 some cases, distinguish between direct and indirect damages or losses. Typically, Swiss law looks at causation to determine whether the parties – or a judge – can attribute a loss 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 that the parties wish to include or exclude (for instance, loss of profits).

In any case, whether addressing matters of direct loss or indirect loss, Swiss law does not allow exclusion from liability in cases of a party's gross negligence or wilful misconduct. That means that provisions implementing a monetary cap on 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. Loss of data and costs for restoring lost data, for example, also constitute an oft-negotiated item, given 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 statutory law – namely the Swiss Code of Obligations (SCO) – will apply. Therefore, if a contract does not address 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 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.

4.5 Contractual Protections on Data and Cybersecurity

It is expected that the outsourced service provider will offer contractual commitments to certain technical cybersecurity and data security measures. Outsourcing agreements typically discuss topics such as encryption of data in transit and data at rest.

In addition, the "technical and organisational measures" (TOMs) are now an integral part of virtually all outsourcing agreements.

Given the legislative advances in the area of data protection, geographical discussions often arise. The customer indeed needs to know where the provider will store, process and transfer its data. This assessment is also necessary for the customer to assess its regulatory data protection exposure and ensure alignment with its data protection practices.

4.6 Digital Transformation

The use of cloud solutions is advantageous in many respects, particularly as it offers great flexibility and a frequently high level of cyber-resilience. Contracts addressing cloud solutions must nonetheless be specific on the location of the cloud server farms and, by extension, the location of the customer's data and its processing. This is relevant from a data protection standpoint. Certain sector-specific considerations, such as those relevant to the financial sector, may also come into play.

5. HR

5.1 Rules Governing Employee Transfers

Swiss law has rules governing employee transfers that may apply to 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 employees are transferred along with a business or part thereof is transferred, unless they refuse. In case of employee refusal, their employment contract ends upon expiry of the notice period.

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

5.2 Trade Union or Works/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 in **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. This leaves little room for any diverging market practice. The parties will, however, contractually address the financial costs However, the parties will contractually address the financial costs – as well as co-operation and information duties – in the event that employees transfer to the service provider or vice versa at the end of the outsourcing.

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.

5.4 Remote Working

Remote working is generally permissible under Swiss employment law. The technologies involved in remote working often enable the employer to closely monitor employee behaviour; this is legally problematic and generally prohibited.

In various sectors, confidentiality and professional secrecy obligations are a core concern with remote working. Certain technologies and best practices, such as paperless workplaces, VPNs and properly equipped corporate IT systems mean that secrecy concerns can typically be overcome. However, such methods are not a "one-size-fits-all" solution and the implementation of a work-from-home practice calls for significant prior analysis.

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, IT, IP and competition law, dispute resolution and tax law. With more than 250 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 IP, IT and data protection product groups at Walder Wyss Ltd. He regularly advises in complex outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. He also has vast experience in copyright, trade mark and patent law. His work focuses particularly on 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 the pharmaceutical, biotech and medtech sectors.

Jürg Schneider is a partner at Walder Wyss Ltd and head of the Lausanne office. His practice areas include IT, 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 cross-border and international contexts. In addition, he regularly publishes and lectures on IT topics and is a member of several professional organisations. Jürg is a past member of the International Technology Law Association's board of directors and former co-chair of its data protection committee.

Hugh Reeves is a managing associate in the IP, IT and data protection product groups at Walder Wyss Ltd. He advises clients in matters of technology transactions, commercial contracts, telecommunications, IP and digitalisation. In addition, Hugh is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion in the Swiss market.

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

Trends and Developments

Contributed by:
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss Ltd see p.20

Introduction

Accurately identifying trends in the Swiss outsourcing field is a delicate exercise. Undeniably, there have been certain sustained market practices that have proved consistent throughout the years and will remain relevant in the future. 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 – both in Switzerland and abroad – and growing suspicions linked to certain technologies or their providers.

Additionally, the deteriorated post-pandemic global geopolitical situation – in particular, the war in Ukraine – has created new challenges that are hampering economic recovery and impacting how Swiss companies do business.

Digital Transformation

Until early 2020, the biggest impact on the outsourcing industry came from new technologies, especially those related to cloud computing, AI and big data. Other technologies or business practices had also been enjoying a growing disruptive influence, as was the case with the blockchain (also known as distributed ledger technology) and the "internet of things" (IoT).

Such a 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 does not necessarily involve any actual outsourcing, as companies may implement these changes internally – for example, by onboarding a new cloud service on a software as a service (SaaS) delivery model.

The process of digital transformation does, however, bear a striking resemblance to outsourcing in its end result, as it allows the customer to streamline business, optimise resource allocation and generally increase efficiency. Moreover, the contracting set-up is in some ways comparable to a conventional outsourcing structure. Both typically involve a master services agreement and schedules featuring various key performance indicators (KPIs), technical and data security requirements, and so forth.

Noteworthy differentiators in the new style of contracts include 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 instead retain their option to move to another provider (eg, a new and more advantageous rival technology).

Conversely, on the provider side, the approach seems to be geared around the avoidance of customer termination. This is usually pursued through automatic contract renewal, few business continuity commitments in case of termi-

nation, long termination notice periods, and so forth.

The above-mentioned trends continue at the time of writing and are expected to gain further traction as companies look to remain at the forefront of technological evolution, either in response to a fear of missing out, commercial considerations or a purely marketing perspective. Although traditional outsourcing is still an absolutely valid and relevant way for companies to focus solely on their core competencies, the counter-current – ie, retaining or insourcing secondary competencies or functions – applies as well and is expected to increase in popularity.

COVID-19 and 5G Technology Providers

Nearly all businesses are now questioning their approach to outsourcing or onboarding third-party technologies in response to:

- the COVID-19 pandemic (and the digitalisation linked thereto); and
- various disputes concerning the safety or reliability of certain offshore providers.

Post-pandemic business models

Firstly, as a result of the economic fallout from the pandemic, Swiss companies have been forced to rethink their business models. They are frequently finding ways to reduce their overhead and operating expenses further.

Many businesses have reassessed their practices in light of the aforementioned tension between:

- the historical benefits of outsourcing to providers based abroad in order to retain only predefined core competencies; and
- the perceived added value in achieving a holistic digital transformation that would onboard certain new technologies and services rather than reallocate them to a third party.

The post-pandemic economic, social and political landscape also means businesses face supply chain difficulties, limitations in international trade and higher inflation and operational costs. 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 identify any clear trend and no consistent momentum has yet emerged.

Reliance on international service providers

Secondly, there have been questions concerning the reliance on certain IT services providers. One much-discussed example is a multinational Asian 5G technology provider that has come under scrutiny in North America and Europe for its alleged ties with the government. Essential 5G technologies constitute critical infrastructures, as national means of communications rely on them. Therefore, many governments have had to take a stance on this important multinational player in the field's admissibility as a provider.

The Swiss government has not imposed any limitation on the reliance on any of the international service providers or their products and services. Ultimately, however, this international scrutiny of an important IT provider has led many companies (of all sizes) to rethink their outsourcing practices because 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 purposes of this article, "nearshoring" can be defined as outsourcing to a provider located in

a neighbouring country or a country that is considered close from a geographical and cultural perspective.

The preference for nearshoring is reinforced by the stringent data protection requirements applicable to Swiss-based companies, as well as certain sectoral rules and guidelines (eg, in the banking sector). Both often lead Swiss companies to remain cautious when outsourcing to or acquiring services from providers based outside the EU or even outside 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 service providers looking to offer their services to Swiss customers frequently have to assess their services under a Swiss telecommunications regulatory lens.

On 25 September 2020, the Swiss Parliament adopted the final text of the draft revised Federal Data Protection Act (FDPA). This revised FDPA, which will enter into force on 1 September 2023, is generally consistent and in line with the requirements of the EU's General Data Protection Regulation (GDPR). Although the revised FDPA does not stray far from the (currently in force) FDPA, it will:

- increased legal obligations on data controllers and processors alike; and
- empower the Swiss authorities to levy more significant fines than is currently the case (CHF 250,000 compared to a maximum fine of CHF 10,000 in certain – limited – circumstances).

The EU and Switzerland both invalidated (either expressly or, in the case of Switzerland, effectively) the Privacy Shield framework in July and September 2020 respectively. The EU issued new, revised "standard contractual clauses (SCCs)" that were recognised by the Swiss data protection authority, provided that the necessary adaptations and amendments are made for use under Swiss data protection law.

However, the fall of the Privacy Shield framework requires Swiss-based companies to check by means of a risk assessment whether their current outsourcing practices remain in line with data protection requirements if they they use service providers based in countries where there the personal data processed by such providers is not adequately protected. Depending on the result of such risk assessment, current outsourcing practices may need to be adapted in a number of ways, including:

- by contractual changes
- by technical means such as encryption and/or pseudonymisation; or
- by changing the service location.

"Local" Outsourced Services

In light of all these considerations, and the shifting geopolitical landscape resulting from the war in Ukraine, there seem to be several arguments in favour of a more "local" sourcing of outsourced services. This is reflected in the approach of several key players (and outsourcing customers) in the Swiss market, who have

come to expect more geographic proximity from their contractual partners.

Nowhere is this more true than in the banking and finance sector. The banking industry and its prudential authority (FINMA) have issued various texts, recommendations, circulars and guidelines that specifically look to facilitate bank outsourcing activities, including to service providers located outside Switzerland.

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

Conclusion

In summary, 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 that customers will 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 post-pandemic world. Therefore, rather than attempting to follow current trends, one should look out for creative yet carefully analysed approaches to outsourcing – both from the customer perspective and the service provider perspective.

Contributed by: Michael Isler, Jürg Schneider and Hugh Reeves, **Walder Wyss Ltd**

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, IT, IP and competition law, dispute resolution and tax law. With more than 250 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 IP, IT and data protection product groups at Walder Wyss Ltd. He regularly advises in complex outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. He also has vast experience in copyright, trade mark and patent law. His work focuses particularly on 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 the pharmaceutical, biotech and medtech sectors.

Jürg Schneider is a partner at Walder Wyss Ltd and head of the Lausanne office. His practice areas include IT, 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 cross-border and international contexts. In addition, he regularly publishes and lectures on IT topics and is a member of several professional organisations. Jürg is a past member of the International Technology Law Association's board of directors and former co-chair of its data protection committee.

Hugh Reeves is a managing associate in the IP, IT and data protection product groups at Walder Wyss Ltd. He advises clients in matters of technology transactions, commercial contracts, telecommunications, IP and digitalisation. In addition, Hugh is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion in the Swiss market.

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

CHAMBERS GLOBAL PRACTICE GUIDES

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

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