Cloud Computing 2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2017
Fifth edition
ISBN 978-1-83862-634-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Cloud Computing
2022

Contributing editors
Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston
Bryan Cave Leighton Paisner LLP

Lexology Getting The Deal Through is delighted to publish the fifth edition of *Cloud Computing*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Marcus Pearl, Sean Christy, Chuck Hollis and Derek Johnston of Bryan Cave Leighton Paisner LLP, for their assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
September 2021

Contents

Switzerland

Oliver M Brupbacher, Ralph Gramigna and Nicolas Mosimann

Kellerhals Carrard

MARKET OVERVIEW

Kinds of transaction

1 | What kinds of cloud computing transactions take place in your jurisdiction?

As Switzerland is experiencing fast changes regarding the demand for services and the underlying technologies, cloud computing adoption has experienced a considerable rate of expansion in this country. The service models of infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) are currently growing at around 20 per cent year over year, exceeding the global growth rate of around 14 per cent, as Swiss enterprises are pushing customer relationship management, unified communications as well as enterprise resource planning to the cloud. Platform-as-a-service (PaaS) is on the rise, too, thanks to the growth in local application development. Rising volumes of data generated by customers and other sources (artificial intelligence, internet of things, edge technology, etc) prompt Swiss enterprises to consider public cloud services and, due to local legal and regulatory compliance considerations, also private and hybrid cloud solutions.

Distinctive features of the cloud computing market in Switzerland include the heightened sensitivity of Swiss enterprises in relation to data localisation laws, data protection and data secrecy, and other regulatory requirements that affect cross-border data transfers (eg, in banking and the healthcare industry). Accordingly, it appears that Swiss companies are focused more on data centre locations, data security, managed services support and contract flexibility when looking for cloud providers, rather than on the portfolio of features offered. In that sense, the availability of local data storage, which is now available from top hyperscalers (ie, entities that can provide cloud, networking, and internet services at scale via IaaS models), has made a major contribution to the growth of cloud computing in Switzerland.

The growing importance of digital transformation is reflected in recent transaction activity. While more and more providers enter the market, there is also a parallel trend towards consolidation with smaller providers being merged into larger system integrators. Transactions in 2020 generally highlight the importance of digital end-to-end process capabilities and vertical integrations, including Insight Partners' acquisition of Veeam for US$5 billion and NEC Corporation's acquisition of Avaloq Group AG for US$2.226 billion (Deloitte, Data centres in Switzerland: Dynamic market awaiting consolidation 2020; KPMG, Clarity on Mergers & Acquisitions 2020).

Active global providers

2 | Who are the global international cloud providers active in your jurisdiction?

The most significant global public cloud providers in Switzerland are Amazon Web Services (AWS), Google, IBM, Microsoft (Azure), Oracle and SAP. Google, Microsoft and Oracle also have cloud regions in the country.

Active local providers

3 | Name the local cloud providers established and active in your jurisdiction. What cloud services do they provide?

Leading national cloud providers include ABACUS, Aveniq, Bechtle, Bexio, Brainserve, ELCA, myfactory, Netcloud, Safehost, Swisscom and VSHN.

As companies shift more of their business-critical operations to the cloud, their storage requirements are reduced, and remaining systems are often moved to co-location. Pure hosting without additional services is rarely profitable enough. Accordingly, local cloud providers increasingly focus on managed services and managed hosting, offering an as-a-service business model to mainly small and medium-sized enterprises. Owing to local legal and regulatory compliance requirements, local providers regularly offer private or hybrid cloud solutions.

Market size

4 | How well established is cloud computing? What is the size of the cloud computing market in your jurisdiction?

Switzerland consistently ranks as one of the most attractive locations for data centres, offering a series of locational advantages, such as a position at the centre of Europe, secure internet infrastructure, strong connectivity, security of power supply, a reputation for technical innovation, high data protection and a stable political environment (Cushman & Wakefield, Data Center Global Market Comparison 2021).

The Swiss data centre market is currently calculated at around US$1.6 billion per year. Its growth is estimated at a compound annual growth rate of over 3 per cent during the period 2020 to 2025.

Impact studies

5 | Are data and studies on the impact of cloud computing in your jurisdiction publicly available?

Information Services Group (ISG) regularly publishes detailed reports on the Swiss cloud computing market (eg, Next-Gen Private/Hybrid Cloud – Data Center Services & Solutions – Switzerland 2021; Public Cloud – Solutions & Service Partners – Switzerland 2020).

Business Wire recently published a report on the Switzerland Data Center Market – Investment Analysis and Growth Opportunities.

In 2019, the Organisation for Economic Co-operation and Development Economic Survey Switzerland analysed the country's technological transformation, including its adoption of enabling technologies, such as cloud computing.

All these reports have been consulted for the present market overview.

POLICY

Encouragement of cloud computing

6 Does government policy encourage the development of your jurisdiction as a cloud computing centre for the domestic market or to provide cloud services to foreign customers?

The Federal IT Steering Unit (FITSU), which ensures implementation of the information and communication technologies (ICT) strategy in the Swiss Federal Administration, adopted a Cloud Strategy. The strategy is primarily addressed at public authorities, but also at interested business circles, in particular cloud providers. It aims at identifying measures to deal with the emerging possibilities and risks in connection with cloud computing.

The Swiss Federal Data Protection and Information Commissioner has published a Guide to Cloud Computing that explains both the risks and the data protection requirements in connection with the use of cloud computing services.

Incentives

7 Are there fiscal or customs incentives, development grants or other government incentives to promote cloud computing operations in your jurisdiction?

No.

LEGISLATION AND REGULATION

Recognition of concept

8 Is cloud computing specifically recognised and provided for in your legal system? If so, how?

Switzerland, in general, pursues a technology-neutral approach to its laws and regulations. The supervisory laws also adopt a neutral and principle-based position regarding technological developments and business models.

The aim is to neither provide undue benefits nor to introduce disadvantages to either old or new technology. However, the fast-developing digitalisation has made it necessary to provide a legislative framework in certain areas, which allows the implementation of new business models. As an example, at the end of 2019, the Swiss Federal Council adopted the dispatch on the further improvement of the framework conditions for distributed ledger technology (DLT). The report showed that Switzerland's current legal framework is already well suited to dealing with new technologies, including DLT. Consequently, the Federal Council refrained from drawing up a specific technology act.

Cloud computing is principally dealt with in commercial contracts and, therefore, governed by contract law, which is regulated under the Swiss Code of Obligations. Additionally, specific aspects and issues are addressed in numerous other laws and provisions. Further, a revision of the Federal Act on Data Protection of 19 June 1992 has been adopted in parliament, and it will be aligned in scope with the EU General Data Protection Regulation. It is expected to be put in force in 2022. The revised Act will have an impact on cloud computing, but not directly address specific cloud topics.

As a result, Switzerland has not introduced any laws and regulations that specifically recognise, and provide for, cloud computing. However, there are sector-specific guidelines and expert opinions that address cloud computing and are nonetheless nonbinding from a legal perspective. For example, the Swiss Bankers Association has drawn up a set of legal and regulatory guidelines for the use of cloud services by banks and securities dealers. These guidelines contain recommendations for institutions and cloud providers on the procurement and use of cloud services. The Swiss Bar Association also published a guideline, expert opinions and minimal requirements to support law firms when using cloud services.

Governing legislation

9 Does legislation or regulation directly and specifically prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

No.

10 What legislation or regulation may indirectly prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Cloud computing is provided and procured on the basis of commercial contracts. Swiss contract law is flexible and allows for coverage of all of the service models available within cloud computing. However, there are numerous laws and regulations imposing requirements, mainly related to the IT-security protection objectives, pertaining to availability, integrity and confidentiality.

Professional confidentiality (professional secrecies, such as banking secrecy, professional secrecy of the lawyer, medical secrecy), business or trade secrecy, and cross-border data transfer restrictions

According to article 321 of the Swiss Criminal Code, any person acting within the capacity of a member of the clergy, lawyer, defence lawyer, notary, patent attorney, auditor subject to a duty of confidentiality under the Swiss Code of Obligations, doctor, dentist, chiropractor, pharmacist, midwife, psychologist, nurse, physiotherapist, occupational therapist, dietician, optometrist, osteopath, or as an assistant to any of the foregoing persons must not disclose confidential information that has been confided to them in their professional capacity, or which has come to their knowledge in the practice of their profession, to an unauthorised third person.

Banking secrecy, according to article 47 of the Banking Act, is also categorised as professional confidentiality. Further, business or trade secrets enjoy additional protections under articles 162 and 273 of the Swiss Criminal Code.

While it is the precedent practice that professional confidentiality and business or trade secrecy do not strictly prohibit the employment of cloud services, appropriate safeguards must be implemented. If a cloud provider and its subcontractors do not in actuality obtain knowledge of any protected information and data being processed within the cloud, there is no disclosure of confidential information. However, the responsible professional or owner of the business or trade secret must have put appropriate technical, organisational and contractual measures in place in order to limit the risk of the provider and its subcontractors accessing the information or data. If the provider or its subcontractors have access to protected information, the duty to maintain professional confidentiality or business or trade secrecy will have to be extended and imposed upon the provider and its subcontractors. The Supreme Court has not yet had the opportunity to decide whether the outsourcing to a provider abroad is compliant with the professional confidentiality requirements.

Article 271 of the Swiss Criminal Code sanctions unlawful activities on Swiss territory on behalf of a foreign state. Under particular circumstances, this provision may limit the outsourcing of specific data from Switzerland to a provider abroad, if such data is ordered to be disclosed there during legal proceedings.

Federal Act on the Surveillance of Mail and Telecommunication Traffic

This Act also applies to cloud services providers if they provide derived communication services, such as email or other forms of digital communication, through their cloud platforms. On the request of investigation authorities and the approval of the competent courts, providers of derived communication have to enable surveillance measures within the scope of the warrant and, upon request, must provide marginal data of the transpired telecommunication.

The scope of application of the Act is limited to Switzerland and therefore does not have an impact similar to that of the US CLOUD Act.

Specific regulations applicable to banks and insurance companies

The Swiss Financial Market Supervisory Authority (FINMA) introduced regulatory requirements on outsourcing with the Circular 2018/3 'Outsourcing – banks and insurers'. It is applicable to banks, securities dealers and insurance companies. FINMA aligned the circular to reflect its principle-based approach and drafted it technology-neutral so that financial institutions are able to implement outsourcing requirements while taking their specific business models and risks into consideration. Within this framework, the appropriate allowance must be made for the higher risks resulting from the outsourcing of activities outside Switzerland, especially with regard to company restructuring and resolution in Switzerland, which must be guaranteed. This Circular applies to cloud services procured by banks, securities dealers and insurance companies qualifying as substantial outsourcing in the meaning of the Circular.

The Circular 2008/21 'Operational risks at Banks' includes key international standards for handling operational risks within the Swiss regulatory framework. The term 'operational risks' includes a wide range of events extending from legal cases and fraud offences to incidents involving IT issues. The Circular further specifies the 'Principles for the Sound Management of Operational Risk' issued in June 2011 by the Basel Committee on Banking Supervision as six thematic principles. These principles require that responsibility for the management of operational risks lies with top management. They also require banks to have a systematic approach, systems and controls, reporting and an IT infrastructure that identify, limit and monitor these risks appropriately.

Where necessary, FINMA can, in the future, lay down specific requirements for managing operational risks in certain areas. Since in recent years within Switzerland attention has been drawn to the operational risks involved when handling electronic client data, FINMA has now defined additional rules in Annex 3 to the 2008/21 Circular. Nine principles are thus set out to preserve the confidentiality of electronic client data (ie, those of individuals (private clients)), and to properly manage the risks involved.

Federal Act on Data Protection

The revised Federal Act on Data Protection – which will be put in force during 2022 – applies to the processing of personal information by private persons and by federal authorities. There are numerous requirements that must be complied with, in the course of providing or sourcing cloud services. Personal data must be protected against unauthorised processing through adequate technical and organisational measures. Personal data may not be disclosed abroad if there are significant risks to the privacy of the data subjects associated with the said transfer, in particular owing to the absence of legislation that provides for adequate protection.

Breach of laws

11 What are the consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing?

Breaches of professional confidentiality, of business or trade secrecy and of cross-border data transfer restrictions under articles 321, 162, 273 and 271 of the Swiss Criminal Code are generally punishable with a custodial sentence not exceeding three years or a monetary penalty, or in certain serious cases with a custodial sentence of not less than one year.

Failing to comply with a request of the surveillance office or unauthorised disclosure of a confidential surveillance under the Federal Act on the Surveillance of Mail and Telecommunication Traffic may result in a fine of up to 100,000 Swiss francs, unless the conduct is punishable as a more serious offence under another law.

Consumer protection measures

12 What consumer protection measures apply to cloud computing in your jurisdiction?

From a data protection and privacy perspective, a cloud provider offering his or her services to a consumer (ie, a natural person), will be, as a general rule, the controller in relation to the personal data of the consumer and has therefore a direct responsibility towards the consumer to fulfil the requirements arising out of the applicable data protection laws.

Further, if a cloud provider uses for contracting purposes general terms and conditions, specific restrictions will have to be considered based on the case law of the Swiss Supreme Court. These include the rules of ambiguity and unusualness. In the case of ambiguous wording, pre-formulated general terms and conditions are interpreted against the author of the clauses. If a clause is qualified as unusual, applying an objective interpretation based on the principle of trust, said clause could be declared unenforceable.

According to article 120 of the Swiss Private International Law Act, contracts relating to the provision of ordinary goods and services intended for the personal or family use of the consumer, and which are not associated with the professional or commercial activities of the consumer, shall be governed by the law of the state in which the consumer is habitually resident, if:

- the supplier received the order in that state;
- the conclusion of the contract was preceded in that state by an offer or an advertisement and the consumer performed there the necessary acts to conclude the contract; or
- the consumer was induced by the supplier to go abroad to place his order there.

A choice of law by the parties is not allowed. According to article 114 of the Act, an action brought by a consumer relating to a consumer contract as defined by article 120 may be filed, at the discretion of the consumer, before the Swiss court at the domicile or, in the absence of domicile, at the place of habitual residence of the consumer; or at the domicile or, in the absence of domicile, at the place of habitual residence of the supplier. The consumer may not waive the venue of their domicile or place of habitual residence in advance.

Sector-specific legislation

13 Describe any sector-specific legislation or regulation that applies to cloud computing transactions in your jurisdiction.

The professional confidentiality set out in article 321 of the Swiss Criminal Code applies to the medical, legal and auditing sectors. Banks

must comply with the banking secrecy regulations. Banks and insurance companies have to implement the requirements imposed by FINMA (Circular 2018/3 Outsourcing – banks and insurers and Circular 2008/21 Operational risks at Banks).

Insolvency laws

14 Outline the insolvency laws that apply generally or specifically in relation to cloud computing.

In general, the Swiss Debt Enforcement and Bankruptcy Act applies in case of the insolvency of a cloud provider or its client. If a contract covering cloud services is not continued by the bankruptcy estate, segregation of physical objects in the possession of the bankruptcy estate, but owned by a third party, can be claimed.

In 2019, the Federal Council initiated a consultation on the adaptation of federal law to the developments in distributed ledger technology. One of the proposals includes a new article 242b of the Swiss Debt Enforcement and Bankruptcy Act. This provision provides a right to access the data under the control of an estate in bankruptcy if a third party can prove a statutory or contractual entitlement to the data. Costs associated with the access will have to be borne by the party requesting access to the data. The provision came into force on 1 August 2021.

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

15 Identify the principal data protection or privacy legislation applicable to cloud computing in your jurisdiction.

To be able to determine the specific duties under the applicable data protection and privacy legislation, it is important to identify the roles of the respective parties. In the case in which a cloud service is offered to natural persons for their own private purposes, the cloud provider acts as a controller, since the provider determines the purposes and means of processing of personal data in relation to these persons. If, however, a company processes client or employee data in the cloud as a controller, the cloud service provider qualifies as a processor.

The revised Federal Act on Data Protection – which will be put in force during 2022 – applies to the processing of personal information by private persons and by federal authorities. There are numerous requirements that must be complied with, in the course of providing or sourcing cloud services. Personal data must be protected against unauthorised processing through adequate technical and organisational measures. Personal data may not be disclosed abroad if there are significant risks to the privacy of the data subjects associated with the said transfer, in particular owing to the absence of legislation that provides for adequate protection. The Federal Data Protection and Information Commissioner has published a list of countries that offer adequate levels of data protection, and the transfer or disclosure of data to such countries is permitted. In the absence of legislation that provides for adequate protection, personal data may only be disclosed abroad if specific conditions are met, such as if sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad. Other grounds for a transfer or disclosure include:

- the consent of the data subject;
- vital interests;
- contractual necessity;
- overriding public interest; or
- the establishment, exercise or enforcement of legal claims before courts, if:
    - the data subject has made the data generally accessible and has not expressly prohibited its processing; or
    - on the basis of binding corporate rules.

A processor may only process personal information on the basis of a contract with the controller and only in the manner permitted by the controller, and as long as such processing is not prohibited by a statutory or contractual duty of confidentiality.

On the cantonal level, cantonal data protection and privacy legislation apply to the processing of personal data by cantonal authorities.

The EU General Data Protection Regulation may apply to cloud service providers or other controllers domiciled in Switzerland by virtue of its article 3. In particular, the regulation applies to the processing of personal data of data subjects, including those in Switzerland, in the context of the activities of an establishment of a controller or processor in the European Union, regardless of whether or not the processing takes place in the European Union. It also applies to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the European Union (such as in Switzerland), where the processing activities are related to the offering of goods or services to such data subjects in the European Union or the monitoring of their cloud computing contracts.

Lastly, according to article 139 of the Swiss Private International Law Act claims based on an infringement of personality rights through the processing of personal data, and claims founded on impairment of the right to information concerning personal data shall be governed, at the discretion of the injured party, by:

- the law of the country in which the injured party has its place of habitual residence, if the injuring party should have foreseen that the effects would occur in that country;
- the law of the country in which the injuring party has its place of business or place of habitual residence; or
- the law of the state in which the effects of the infringement have occurred if the injuring party should have foreseen that the effects would occur in that state.

As a result, and depending on the specific circumstances, data protection or privacy legislation of other jurisdictions may apply in Switzerland.

CLOUD COMPUTING CONTRACTS

Types of contract

16 What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

Currently, contracts predominately regulate software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS) and anything as a service (XaaS). While companies are customers under all these different forms of cloud contracts, consumers typically only enter into contracts for SaaS and PaaS solutions, in particular for cloud storage services offered by providers such as Dropbox and Apple.

As regards SaaS contracts in particular, a customer will enter into a service agreement with either a national or international provider; however, these SaaS providers often do not have their own cloud infrastructure and thus use either global or national cloud providers as subcontractors.

The agreements with the global providers are often standardised and more often than not presented on a non-negotiable basis to their consumers and business customers. The same is generally to be observed in agreements with the national providers that offer standardised service packets. Although the agreements are often presented as being standardised and non-negotiable, they are often nevertheless, if only partly, negotiable. Additionally, providers frequently use general terms and conditions for their agreements, some of which only provide said terms electronically.

Swiss law in general is conducted under the principle of freedom of contract, and there are only limited restrictions to this principle. The agreements that are governed by Swiss law often resemble those of the United Kingdom and the United States in style and content, albeit a bit shorter.

Cloud agreements in regard to SaaS, PaaS, IaaS and XaaS agreements typically comprise various elements of statutorily regulated types of contracts, among which are contracts for work and services, service agreements and rental agreements, but they also contain elements of contract types that are not regulated by the Code of Obligations (in particular licence agreements).

Typical terms for governing law

17 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

The Swiss Private International Law Act governs international jurisdiction and the applicable law, provided that no treaties (eg, the Lugano Convention) apply. According to this Act, parties are generally at liberty to agree upon a governing law. In practice, Swiss national providers and customers having the requisite negotiating power will typically insist on Swiss law as the governing law of the contract, while international providers will insist on the law applicable where they hold their registered office. Often enough, however, US providers with a certain level of establishment within the European Union may accept the designation of the law of an EU member state or of Switzerland. In international agreements, parties tend to agree upon the jurisdiction that coincides with the chosen governing law. The Swiss Private International Law Act and the Lugano Convention further contain rules on the enforcement of foreign court rulings within Switzerland respectively the enforcement of Swiss rulings in other Convention member states.

Typical terms of service

18 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

A standard agreement regulating the provision of SaaS, PaaS, IaaS and XaaS will include the terms on:

- the licence or right to use the service;
- obligations of the customer, such as user restrictions in general and in particular acceptable use policy;
- obligations of provider, such as meeting specific service levels (eg, with regard to response times, problem-solving, uptime or availability of service, if applicable) or just using best efforts only to provide the service;
- security, business continuity and disaster recovery;
- the provider's right to temporarily suspend the services either in the case of customer's breach of the agreement or at the provider's sole discretion;
- payment of fees;
- warranties, in particular of provider, and remedies, whereby providers are typically trying to exclude all statutory rights of the customer (eg, the right to reduce the fees) and instead grant the customer the right to request that the issue is solved;
- exclusion of liability for loss of data and indirect or consecutive damage, such as lost profits and limitation of any other liability (in particular for direct damage) to a specific aggregate amount, all the aforesaid to the extent permitted by law;
- force majeure, whereby events that could have been prevented by reasonable measures are typically not considered a force majeure;
- intellectual property rights;
- confidentiality, data protection and cybersecurity requirements;
- term of the agreement, its termination and effects of termination (such as deletion of hosted data); and
- governing law and jurisdiction.

Typical terms covering data protection

19 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

The terms will be drafted in compliance with all of the potentially applicable data protection laws (ie, in most cases the federal or cantonal data protection laws and the EU General Data Protection Regulation (GDPR)) in mind, often in the form of the reiteration of the requirements of said laws. To comply with the data protection laws, it will generally be clearly stated which party is the controller and which is the processor, and these roles and their duties will be clearly defined.

The agreements often contain rules on cross-border transfers of data and on the provider's right to use sub-processors to fulfil its contractual duties. Additionally, the provider's obligation to follow the customer's instructions when processing data, and the duty to abide by the technical and organisational measures agreed upon, which are generally incorporated into an annex, are also terms of the agreement.

There are typically obligations to enter into a separate data processing agreement, sometimes on the basis of EU standard contractual clauses.

Sometimes, the customer's audit rights or the obligation of the provider to uphold and comply with ISO certificates (in particular ISO 27001) will also be included as a term of the agreement.

Typical terms covering liability

20 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

The liability terms will often exclude all liability to the fullest extent permitted by law (ie, no liability save for wilful intent and gross negligence and in cases of personal harm, the latter of which lacks relevance in most of these agreements). In most cases, indirect damage, lost profits, loss of data etc, will be excluded as far as possible. If liability for direct damage is not excluded in its entirety, the parties will usually agree to limit the amount payable to a specific amount (eg, one or two times the annual fees to be paid by the customer). If the provider commits to meet certain key performance indicators according to a service-level agreement (eg, response times, availability of the services, time to remedy errors, etc), non-fulfilment usually results in service credits and not liability. The amounts of these service credits are often quite low and not particularly relevant.

Indemnity for the provider as a result of third-party violations of customer data is also generally included within the terms of the agreement.

Typical terms covering IP rights

21 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

Cloud computing contracts often clarify that each party remains the owner of its intellectual property rights and no intellectual property

rights are transferred from one party to the other. This, in particular, concerns the customer's data that is hosted by the provider but also the provider's intellectual property rights relating to the service or involved software.

Business-to-business (B2B) contracts usually contain obligations of the provider to indemnify the customer from infringements of third-party rights as a result of the customer's use of the service.

Typical terms covering termination

22 What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

Most B2B cloud computing contracts are concluded for a fixed term and thus may only be terminated early by a party on the basis of specific reasons (eg, a material breach of the agreement by the other party, the bankruptcy of the other party or a change of control). Notice periods for a termination do not need to be identical for the parties (eg, the notice period for a termination by the provider could be longer to enable the customer to find an alternative solution).

Upon termination of the agreement, the customer may typically no longer use the service, while the provider is obliged to transfer all customer data to the customer or a third party in a standard computer-readable format. Moreover, the provider could be obliged to cooperate in the orderly wind-down of the services that are terminated or transitioned back to the customer or to another service provider, either at no additional cost or at predefined rates.

Employment law considerations

23 Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

If the customer uses the provider's service to process the personal data of the customer's employees (eg, storage of records of employees), the customer is obliged to comply with article 328b of the Code of Obligations and the applicable data protection laws.

If within the context of the cloud computing contract, the customer's business or part of its business is transferred, article 333 of the Code of Obligations could apply. According to article 333, among other things, the relevant employee's contractual relationships automatically transfer together with the business.

TAXATION

Applicable tax rules

24 Outline the taxation rules that apply to the establishment and operation of cloud computing companies in your jurisdiction.

Cloud computing companies based in Switzerland (effective place of management) are subjected to Swiss profit and capital taxation. Their entire profit and (net) assets are generally subject to Swiss taxes (unlimited tax liability), except the profits and assets attributable to a permanent establishment (or real estate) abroad. At the establishment of a Swiss legal entity, stamp duties might become due (depending on the legal form and the initial capital).

Cloud computing companies based abroad (effective place of management) are also subject to Swiss profit and capital taxation, if they have a permanent establishment in Switzerland. In such cases, only the profits and assets attributable to the permanent establishment are subjected to Swiss taxation (limited tax liability).

In any case of international activity of a Swiss company or a foreign company with a permanent establishment in Switzerland, the applicable double taxation treaty (if any) has to be considered.

The question of whether or not the activity of a cloud computing company creates a permanent establishment for tax purposes is assessed on a case-by-case basis. The Organisation for Economic Co-operation and Development Model Tax Convention Commentary and the international jurisprudence may be considered regarding such assessment.

Indirect taxes

25 Outline the indirect taxes imposed in your jurisdiction that apply to the provision from within, or importing of cloud computing services from outside, your jurisdiction.

Cloud computing services are subject to Swiss value-added tax (VAT) if the beneficiary of the service is located in Switzerland (permanent establishment). The applicable tax rate currently amounts to 7.7 per cent. Generally, any company headquartered in Switzerland that has an annual turnover exceeding 100,000 Swiss francs from taxable services provided either in Switzerland or abroad is subject to Swiss VAT and obliged to register with the Swiss VAT register. In principle, the same condition applies to companies headquartered abroad.

Companies that only provide cloud computing services to customers domiciled in Switzerland are not obliged to register with the Swiss VAT register. If a cloud computing provider is not registered, the customers domiciled in Switzerland have to declare and pay VAT themselves (service import tax) if they are subjected to VAT anyway or if they are recipients of taxable services from abroad in the amount of 100,000 Swiss francs or more.

RECENT CASES

Notable cases

26 Identify and give details of any notable cases, or commercial, private, administrative or regulatory determinations within the past three years in your jurisdiction that have directly involved cloud computing as a business model.

The Federal Supreme Court has clarified that data stored on cloud servers is amenable to search and seizure measures in accordance with the provisions for gathering evidence under the Swiss Criminal Procedure Code, including when the servers are located abroad. It further ruled that such data hosted on foreign cloud servers is not considered evidence on a foreign territory and does not need to be gathered via international mutual legal assistance proceedings, as long as it is accessible via a domestic internet connection and provider.

UPDATE AND TRENDS

Key developments of the past year

27 What are the main challenges facing cloud computing within, from or to your jurisdiction? Are there any draft laws or legislative initiatives specific to cloud computing that are being developed or are contemplated?

As a consequence of the coronavirus pandemic and the associated lockdown, new remote workplaces and workplace services have been rolled out, and digital shops and bank trading desks experienced significantly stronger demand. According to ISG (Next-Gen Private/Hybrid Cloud – Data Centre Services and Solutions – Switzerland 2021), the number of market participants that want to be supplied with a latency of 35 milliseconds or less rose sharply in 2021, putting the underlying infrastructure and supply to the test and presenting new challenges with respect to service-level agreement performance.

A survey conducted in 2020 concluded that there is no need for a 'Swiss Cloud', in the form of an independent technical infrastructure subject to public law, as a factor for success for Switzerland as a business location. However, the potential users emphasised a strong support for 'Swiss Cloud' as a label for the secure use of cloud services that meet the special requirements of data sovereignty. The survey further concluded that there is a need for clarity on legal issues, especially on the inclusion of Switzerland in European cloud initiatives, on common basic cloud services for a Swiss digital administration, and on guaranteeing immunity for the data of international organisations.

In response to these findings, the Federal Council intends to conduct a detailed examination of further aspects, including a certification system for cloud services, the need for crisis-resistant services, international networking, and Switzerland's positioning as a location for data storage.

In June 2021, four US providers (Amazon, IBM, Oracle and Microsoft) and Chinese player Alibaba won a public tender for cloud services in the total amount of 110 million Swiss francs. Swiss companies were not able to score as the public tender was targeted at global cloud players. According to the Federal authorities, the five selected providers were mainly chosen because of the attractive prices offered. Some newspapers and commentators criticised the decision to outsource government data to foreign cloud providers due to privacy concerns.

Google, which came away from the process empty-handed, filed an appeal against the decision, which is currently being examined by the Federal Administrative Court.

Kellerhals Carrard

Oliver M Brupbacher
oliver.brupbacher@kellerhals-carrard.ch

Ralph Gramigna
ralph.gramigna@kellerhals-carrard.ch

Nicolas Mosimann
nicolas.mosimann@kellerhals-carrard.ch

Henric Petri-Strasse 35
PO Box 257
4010 Basel
Switzerland
Tel: +41 58 200 30 00

Raemistrasse 5
PO Box
8024 Zurich
Switzerland
Tel: +41 58 200 39 00

www.kellerhals-carrard.ch

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-634-1