Cloud Computing 2020

Contributing editor
Mark Lewis

LEXOLOGY®
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House
34–35 Farringdon Street
London, EC4A 4HL
United Kingdom

First published 2017
Third edition
ISBN 978-1-83862-164-3

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

Cloud Computing
2020

Contributing editor
Mark Lewis
Bryan Cave Leighton Paisner LLP

Lexology Getting The Deal Through is delighted to publish the third 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. Our coverage this year includes a new chapter on Austria.

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 editor Mark Lewis of Bryan Cave Leighton Paisner LLP, for his continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
October 2019

Contents

Global overview

Mark Lewis
Bryan Cave Leighton Paisner LLP

It took from November 2009 to September 2011 and 15 drafts for the US National Institute of Standards and Technology (NIST) to produce its final definition of cloud computing. (For the short story of that journey, see www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published, and for the final version of the definition, see The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Peter Mell and Timothy Grance, Special Publication 800-145 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.) It was worth the wait, because in practice the NIST definition remains the definitive universal statement of what cloud computing is.

In the time it took the NIST to produce 15 drafts and release a final version of the world's favourite cloud computing definition, the global public cloud services market had grown from US$58.6 billion to US$92.97 billion by revenue (58.65 per cent). By 2018, global public cloud services revenue had almost doubled to US$182.4 billion. During 2019, worldwide revenue is expected to reach US$214.3 billion (17.49 per cent growth). And by 2022, it is predicted to have surged to US$331.2 billion (54.55 per cent up on 2019) – three times the growth of overall global IT services revenues during that period. (See Gartner Forecasts Worldwide Public Cloud Revenue to Grow by 17.5 Percent in 2019, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.) These metrics demonstrate that public cloud computing has not just come of age – it is becoming the norm in computing models.

To return to the NIST's definition of cloud computing, arranged over just one and a half pages, it is:

> *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

The three NIST service models are: software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). TechMarketView, a UK software and IT services industry analyst, has proposed two useful additions to the NIST service models: business process-as-a-service (BPaaS) – an IT-enabled business service delivered from a SaaS platform – and application-as-a-service (AaaS). In their view, it is important to distinguish between software delivered as a service by proprietary software houses and SaaS provided by IT service providers. Accordingly, in their definition, AaaS is SaaS delivered by IT service providers.

The four NIST deployment models are: private cloud, community cloud, public cloud and hybrid cloud. In general, what most people mean when they refer generically to cloud computing is the third deployment model, which is often seen as the archetypal cloud (ie, the public cloud):

> *the cloud infrastructure . . . provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider. (NIST definition, page 3)*

It is the cloud model for which the most extensive claims are made in this computing model: utility, multi-client, location neutral, almost infinitely scalable and pay-per-use (see 'Essential Characteristics', NIST definition, page 2).

But migrating from 'traditional' computing models to the public cloud has real challenges: chief information officers (CIOs), chief information security officers (CISOs) and chief risk officers (CROs) worry about, among others, cybersecurity, compliance with data protection and privacy laws, data residency, service resilience and portability of data on termination of cloud arrangements. So, to avail themselves of some of the benefits of the archetypal cloud, organisations have deployed instead the hybrid cloud: an infrastructure composed of 'two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (eg, cloud bursting for load balancing between clouds)'. (NIST definition, page 3.)

Hybrid cloud is not without its challenges, but it reflects a more measured approach. Organisations that are even more concerned about risk and compliance (eg, regulated financial services firms), but that want some of the benefits of the computing model, are likely to deploy a private cloud, which is 'provisioned for exclusive use by a single organisation comprising multiple consumers (eg, business units). It may be owned, managed and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises'. (NIST definition, page 3.) Alternatively, in a community of common interests, for example within local government, health and law enforcement communities, they may deploy a community cloud:

> *provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg, mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. (NIST definition, page 3)*

As the community cloud shares the characteristic of 'exclusive use' with the private cloud deployment model, we may treat it as a variant of the private cloud for the purposes of this work.

The four deployment models are currently in use, but to varying degrees. For the reasons given below, in our analysis of how cloud computing has been adopted in the countries covered by this work, in general we address the deployment models as a composite of cloud computing – and as virtually interchangeable. This is largely because

locating data to compare and contrast the adoption of each of the deployment models (and for that matter each of the service models) that will be freely available to our readership, while also being authoritative, is a real challenge. And it does not help that, in their endeavours, law and policymakers and regulators have not generally – yet – seen the need to distinguish precisely between each of the cloud deployment and service models. However, where we can do so within the limitations of our allotted space, we try to identify the characteristics of a deployment model that may be relevant to our analysis. Take, for example, the question concerning labour and employment law considerations applicable to the cloud. And in particular, whether the EU Acquired Rights Directive (ARD) and EU member state legislation implementing it will apply to a cloud migration. If that legislation does apply, it will transfer staff automatically on their existing terms of employment to the cloud service provider (CSP) where their employer is migrating some or all in-house IT functions to the cloud. And this will almost certainly extinguish the financial case for the cloud migration. In considering whether there is an ARD transfer of an undertaking, it may well make a difference that the migration is to a public cloud (where you might struggle to discern the transfer of an undertaking, because the 'before and after' activities are so different), rather than to a private cloud (which could have many characteristics of an outsourcing, to which the ARD has been held to apply). Or will it? Readers with business interests in the EU will have to decide for themselves – alerted to the possibility by this work and, one hopes, properly advised.

For the reasons given above, it is mostly beyond the scope of this work to differentiate precisely or at all between and focus on each of SaaS, PaaS and IaaS. Accordingly, in this work we attempt to cover the broadest possible spectrum of cloud computing adoption, including (mostly interchangeably) the public, hybrid and private cloud deployment models and the service models, all in a business-to-business (B2B) context, but recognising that business-to-consumer (B2C) arrangements will also be of interest to many of our readers, mainly because of consumer protection regulation. For each contributing country, this approach will, naturally, be somewhat different, depending on the size and state of development of cloud computing in its local market, as well as local contractual, legal and regulatory conditions.

Our survey starts with the market in each of the countries covered and examines what kinds of cloud computing transactions take place and which of the global and local cloud providers are active in that country, as well as the cloud services the latter provide.

Next, we address how well-established cloud computing is, including by its market size, referring (where practicable) to data and studies that are publicly available.

How active is central or regional government in the development of cloud? Are there specific, cloud-friendly policies? How are those policies implemented – by fiscal or customs incentives or development grants, or other means? And what other government initiatives apply?

We turn next to the core of this work: law, regulation, contract and market practice. We address the following questions for each country.

- Is cloud computing specifically recognised and provided for in the local legal system and, if so, how?
- Is there any legislation or regulation that directly and specifically prohibits, restricts or otherwise governs cloud computing?
- What legislation or regulation indirectly prohibits, restricts or otherwise regulates cloud computing?
- What are the consequences of breach of those laws and regulations?
- Recognising the importance of B2C cloud adoption, what local consumer protection measures apply to cloud computing?
- Knowing that cloud – especially public cloud – may pose real challenges in certain sectors, for example, financial services and health, what (if any) sector-specific legislation or regulation applies?

BRYAN CAVE LEIGHTON PAISNER BCLP

Mark Lewis
mark.lewis@bclplaw.com

Adelaide House
London Bridge
London EC4R 9HA
United Kingdom
Tel: +44 20 3400 1000
Fax: +44 20 3400 1111
www.bclplaw.com

- Public and private sector organisations around the world worry about – and some have already had to cope with – what happens when a CSP becomes insolvent. What insolvency laws will apply in those situations?

Almost all surveys of CIOs, CISOs, CROs and other business leaders around the world highlight their continuing concern about cyber and data security in the cloud, as well as whether and how they continue to comply with data protection and privacy regulation in migrating to the cloud – especially since the coming into operation of the EU General Data Protection Regulation in May 2018. So, we identify the principal data protection or privacy legislation applicable to cloud computing.

We turn next to what I personally have found to be the most challenging set of questions to answer. After outlining what forms of cloud computing contract are usually adopted, we analyse as far as we can from publicly available sources, the typical key terms of B2B public cloud computing contracts in local markets.

It is clear that cloud computing will – if not now, then in the near term – have a significant impact in the workplace, so we also identify labour and employment law considerations that apply.

Because much of the developed world and many emerging economies are becoming increasingly concerned about how to tax online and digital products and services, especially where supplies cross borders and will be made from IT product and services providers without a permanent establishment in their target markets, we outline the direct and indirect taxation rules that apply to the establishment and operation of CSPs and their customer transactions.

Finally, we identify recent notable cases as well as commercial, administrative or regulatory decisions or actions that have directly involved cloud computing as a business model. And we close with a survey of updates and trends as far as they can be discerned.

With a new and fast-developing area such as cloud computing, we must keep our questions under review for future editions. And it follows that our answers to those questions may change over time. Of course, law and regulation will change, as will contract and market practice.

The country contributors and I very much hope that you will find this third edition of *Lexology Getting The Deal Through – Cloud Computing* both stimulating and useful, and a worthwhile addition to this series.

Argentina

Diego Fernández
Marval, O'Farrell & Mairal

MARKET OVERVIEW

Kinds of transaction

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

Almost all kinds of cloud computing transactions take place in the region.

In connection with public cloud services, software-as-a-service (SaaS), infrastructure-as-a-service (Iaas) and platform-as-a-service (PaaS) are all common. Of these segments, SaaShas has had the most marked growth in the recent years. Private cloud models have mostly been adopted by different types of companies.

There has been a growing interest in cloud solutions from the insurance, telecommunications and banking industries. Furthermore, both the national and local governments have begun turning to cloud solutions, in any of these architectures (Saas, IaaS or PaaS).

Active global providers

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

The most common providers operating in Argentina include Oracle, IBM, Microsoft Azure and AWS.

Active local providers

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

Oracle, Microsoft and IBM are the main providers, although not all of them have Saas, Iaas, and Paas as part of their service offering.

Also, most telecommunications companies provide cloud computing capabilities to offer their services to companies and homes. Local companies providing cloud services include Claro, Movistar and ARSAT (a government-owned telecommunications company). The business model is mostly based on providing hosting and offering flexible payment options.

Market size

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

Despite the fact that many companies have already acquired cloud solutions, cloud architecture is today under analysis by different companies as a way to modernise, update or escalate their solutions.

Cloud architecture solutions are being incorporated by new small and medium-sized companies that now have access to world-class solutions. At the same time, cloud services have also been incorporated by large corporations with a need to update their current solutions to be able to escalate and move quickly to more modern solutions.

Impact studies

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

To the best of our knowledge, there are no hard studies with specific numbers. Nevertheless, cloud services allow companies to start new businesses or new operating units in a few months. These are some of the benefits that companies will find when turning to cloud services.

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?

In general, Argentina does not have a federal policy to encourage the development of the country as a cloud computing centre for the domestic market or provide cloud services to foreign customers.

However, Argentina has a law that seeks to foster the growth of the software industry in general and has also recently enacted Law No. 27,506, which provides for a promotional regime for the Knowledge Economy, which aims to promote economic activities that apply the use of knowledge and the digitalisation of information (supported by progress in science and technology) to obtain goods, provision of services or improvements in processes (see question 7).

Furthermore, the Argentine government is involved in cloud computing through ARSAT. ARSAT has constructed a state-of-the-art data centre with the goal of facilitating cloud computing for consumers. The data centre's design and construction has made it the sole Uptime Institute Tier III data centre in Argentina. The data centre has also received ISO/IEC Certification 27001:2013 as well as Communication 'A' 4609 approval from the Argentine Central Bank, both of which certify the rigour of the data centre's information security.

Moreover, despite the fact that there is no formal government law specifically fostering the development of cloud architecture, many industry associations publish different recommendations regarding the cloud.

Incentives

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

Although there are no specific regulations to promote cloud computing in Argentina, the Software Promotion Law No. 25,922 (the Software Law) sets forth a broadly supportive regime for the software industry in general, that will remain in effect until 1 December 2019.

Pursuant to this law, Argentine-incorporated companies whose activities are the creation, design, development, production, implementation, adjustment, or upgrade of developed software systems and their associated documents, may participate in the benefits created by this regime, provided they comply with certain requirements. Beneficiaries of the regime will benefit from:

- fiscal stability;
- conversion of certain monthly social security tax payments into a tax credit;
- non applicability of any VAT withholding or collection regimes;
- a 60 per cent reduction in the total amount of corporate income tax as applied to income derived from software activities; and
- exclusion from any kind of present or future restriction on the currency transfers matching the payouts for imports of software products by the beneficiaries, provided the imported goods are necessary for the software production activities.

Furthermore, the Promotion Regime of Knowledge Economy Law No. 27,506 provides for a promotional regime (the Regime), which will become effective as of 1 January 2020 and will be valid until 1 December 2029. Among others, the regime will benefit the following activities: software, computer and digital services; audiovisual production and post-production; biotechnology, neurotechnology and genetic engineering; geological and prospecting services and others related to electronics and communications; professional services as long as they are exported; nanotechnology and nanoscience; aerospace and satellite industry; nuclear industrial engineering; artificial intelligence, robotic and industrial internet, the internet of things, augmented and virtual reality, etc.

Regarding the tax benefits of the Regime, we highlight the following:

- Fiscal stability: as of the moment of the registration and for the term of validity of the Regime. This benefit may be also extended to provincial and municipal taxes, as long as such jurisdictions adhere to the law.
- Income tax: the general corporate tax rate is reduced to 15 per cent, to the extent that the beneficiaries maintain their payroll. In addition, beneficiaries will be allowed to deduct a tax credit derived from any payment or withholding of foreign taxes, if the taxed income constitutes an Argentine source of income.
- Value added tax (VAT): beneficiaries will not be subject to any withholding and/or collection VAT regimes.
- Employer social security contributions: beneficiaries will be able to fully detract from their employer social security contributions, in relation to each employee, an amount equal to the maximum established in article 4 of Decree 814/2001 (which currently is 17,509.20 pesos).
- Additional benefit: beneficiaries will be able to obtain a one-time transferrable tax credit bond, which can be used for paying advances or balances of income tax or VAT. The bond is equal to 1.6 times the amount of the employer's social security contributions that the beneficiary did not pay due to the benefit mentioned in the above paragraph.

In addition, it is worth noting that, from a customs perspective, cloud computing services may not be construed as a 'good' that may be imported. However, pursuant to a new regulation on the export of services, cloud computing services that are rendered in Argentina but exploited abroad may be construed as an 'export' subject to export duties.

Some specific provisions may apply when importing servers into Argentina, depending on which tariff code they are subject to under the Mercosur Common Nomenclature. These goods are singled out as 'technological goods' and, if imported new, have a reduced VAT rate (10.5 per cent) for their definitive importation, are exempt from the statistical fee (0.5 per cent over cost, insurance and freight (CIF) valuation) and are also exempted from some advanced payments on internal taxation collected upon the definitive importation of goods.

These are also capital goods that, if imported on a used condition, are subject not only to regular import taxation but also to a specific regime that alters their import duties rate (up to twice the import duty rate) and requires a specific certificate granted by the Ministry of Production before its importation. Depending on their tariff position, the importation into Argentina of used servers may be completely forbidden.

LEGISLATION AND REGULATION

Recognition of concept

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

Cloud computing is not recognised or regulated by a specific law.

However, there are different regulations that apply to matters that may relate indirectly to cloud computing, including general provisions on contract law, data protection, consumer protection, labour, intellectual property, tax and public procurement regulations. Taken as a whole, these constitute the framework that would apply to cloud computing.

Governing legislation

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

There is no legislation that directly and specifically prohibits, restricts or otherwise governs cloud computing in Argentina.

Section 8 of the Argentine Digital Law No. 27,078 (the ADL), as amended by Decree 267/2015, establishes that the provision of information, communications and technology services (ICT services) requires a corresponding licence. ICT services are defined by the ADL as the set of resources, tools, equipment, software, applications, networks and means that allow the compilation, processing, storing and transmission of information, such as voice, data, text, video and images, among others. Section 6, subsection (g) of the ADL establishes that each ICT service will be subject to its specific regulatory framework.

At present, there is no specific telecom regulation in Argentina governing cloud computing services. In principle, cloud computing services would not fall under the Argentine telecoms regulations since they would not be an ICT service with specific regulation but merely an application of – or business solution that runs on – the public internet, provided locally by an authorised local internet service provider. Therefore, a reasonable interpretation is that cloud computing services would not be subject to any licensing or other regulatory requirement in Argentina.

Discussions of a new legal framework for telecommunications (and media) activities are still pending. Thus, if such discussions are resumed there may be changes in such regulations in the future and we cannot disregard those changes affecting cloud computing services.

Finally, in connection with personal data protection and regulation of international data transfers, see question 15.

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

There are several provisions that could indirectly restrict or otherwise govern cloud computing, and which could apply depending on the characteristics and nature of the services and the parties involved.

For instance, the Argentine Data Protection Law No. 25,326 will apply to the use of cloud computing insofar as it entails the processing of personal data. The Consumer Protection Law No. 24,240 (the CPL) will also apply to cloud services if they are provided to consumers. Market-specific laws like Decree No. 274/2019 of Fair Trade may also be relevant. Furthermore, general intellectual property, tax and labour regulations should be taken into account.

Breach of laws

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

There are no laws directly prohibiting, restricting or otherwise governing cloud computing. In the case of any laws that may apply indirectly, consequences will vary depending on the pertinent regulation.

For instance, in the case of the Argentine Data Protection Law No. 25,326, a breach may lead to administrative sanctions, civil proceedings, or criminal penalties. The Data Protection Authority (DPA) may apply the following administrative penalties in the event of violation of the Argentine Data Protection Law:

- observation;
- suspension;
- fines of between 1,000 and 100,000 pesos (DPA Rule No. 71 E/2016 capped fines applicable for various infringements encompassed by the same administrative proceeding, stating a maximum cap of 5 million pesos);
- business closure; or
- cancellation of the database.

Sections 117-bis and 157-bis of the Criminal Code also punish, with between one month and three years of imprisonment, those who:

- illegally insert false information in a database;
- knowingly supply false information stored in a database to a third party;
- knowingly and illegally gain access to a database containing personal data in violation of its security systems;
- disclose personal data protected by duty of confidentiality pursuant to law; or
- illegally insert data in a database.

In the case of any infringements of the Consumer Protection Law No. 24,240, the following sanctions:

- observation;
- fines of between 100 and 5 million pesos;
- seizure of infringing merchandise or products;
- business closure or suspension of the provided service for up to 30 days;
- suspension for up to five years from the registries that allow suppliers to contract with the government; and
- loss of concessions, privileges, and any special tax or credit conditions.

Further, the CPL provides that punitive damages may be imposed on the infringer.

Additionally, in case of violation of the Fair Trade Decree, the Authority may impose the following sanctions:

- fines of up to 264 million pesos;
- suspension of licences to contract with the state;
- potential loss of any tax or credit exemptions or benefits; and
- closing of business for up to 30 days.

Consumer protection measures

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

If cloud computing services are provided to consumers, Argentine consumer protection regulations will apply. In particular, the CPL and the provisions of the Civil and Commercial Code (the CCC) on consumer electronic contracts will be relevant.

The CPL protects consumers, defined as any physical person or entity that acquires or uses, whether for a fee or not, goods or services as an end user, for its own benefit or for the benefit of its family or social group.

Some central aspects of general protection consumer law that may be relevant to e-commerce are the following:

- under the CPL, every description of the service or product advertised by any means of communication is considered part of the offer and a binding term of the contract;
- suppliers are forbidden from compelling the consumer to reject goods or service to avoid the payment of a fee (opt-out sales); and
- the CPL entitles the consumer to terminate the contract by the same means used to agree upon it (ie, telephone, internet, etc).

Further, section 40 of the CPL states that there is joint liability between all those involved in the supply chain for damages resulting from defects or risks associated with goods or service.

In addition, the CCC contains provisions that refer specifically to the protection of consumers in electronic transactions (sections 1106-1116). For instance, an important provision is section 1106, which states that electronic means may be used in contracts and have the same force of law as written contracts. Section 1110 CCC grants consumers a 10-day term to revoke the online transaction (with exceptions for: goods that are personalised or that, by their nature, cannot easily be returned; video or audio recordings or software that upon delivery can be quickly and indefinitely stored and copied; and for daily or periodical publications, such as newspapers). Moreover, section 2655 CCC provides that if the cloud computing service located outside offers or advertises the service in Argentina, or performs another activity in Argentina in connection with the proposed contract, and the targeted consumer also performs acts in Argentina addressed at executing the contract, then, Argentine law (CCC and CPL) will apply. In turn, section 2654 CCC states that the court of the place where the consumers perform acts addressed at executing the contract has jurisdiction to hear their claims. Choice of law and jurisdiction clauses will be almost certainly set aside by local courts, which would apply the provisions of the CCC instead.

Sector-specific legislation

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

In the public sector, there is no specific legislation or regulation that applies to cloud computing transactions at a federal level. However, the Federal Information Technology Office – responsible to the Government Secretariat of Modernisation – has approved a Code of Good Practice for the Development of Public Software in the Elaboration, Extension and Improvement of Software Solutions for the Public Sector (Disposition No. 2/2019) (the Code), applicable to the federal public sector. Pursuant to its section 3, all public sector agencies must manifest compliance with the Code every time a software project is carried out.

The Code includes number of recommendations that relate to cloud services, such as:

- the public sector should choose cloud-services solutions over any other option when requesting new information technology services;
- public sector entities will choose which cloud service to procure; and

- providers of cloud services to the public sector will have to comply with certain minimum requirements during the procurement process.

In general terms, public procurement regulations provide for the sanction of particular bidding terms and conditions for each type of procurement. Pursuant to Argentina's political system, the procurement legal framework differs in each jurisdiction and can also vary depending on the relevant entity. The procurement framework at the federal level mainly consists of:

- Decree No. 1023/2001; and
- Decree No. 1030/2016 (together, the General Legal Framework), which provide general rules that cannot be neglected even by way of private negotiation.

Pursuant to the General Legal Framework, it is the public sector that will determine and announce the service that needs to be procured, along with the scope and modalities under which the service will be rendered, by means of the bidding terms and conditions and the technical specifications.

In relation to the banking industry, it is worth noting that in November 2017, the Argentine Central Bank issued Communiques which made important modifications to the regulations which apply to the decentralisation, outsourcing and delegation of activities of financial entities. Among other faculties, these regulations authorised financial entities to hire information technology services provided by third parties, subject to the condition that such activities fall within the list provided by the Argentine Central Bank.

These new rules were an important update to the regulatory framework applicable to financial entities, and aimed to allow them to make a more extensive use of technological services.

Insolvency laws

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

Where a company fails to meet its obligations, the contractual provisions entered into by the parties are the first source of regulation for the conflict. In B2B contracts, where the negotiation leverage is supposedly fairer for the parties, the contract will govern what occurs in cases of non-compliance, which will generally come about if a company becomes insolvent. In B2C contracts, the same contractual provisions will apply with the caveat that, in this case, consumer-specific legislation might apply and might offer more protection to a customer.

In connection with insolvency, general insolvency laws will apply to cloud computing, since there is no specific regulation in connection with insolvency and cloud computing services. The most important Argentine regulation on this matter is the Law on Reorganisation and Bankruptcy Proceedings No. 24,522.

If the reorganisation procedure regulated by this law is successful, the service provider should be able to clear its debts and continue operating. Therefore, the provision of services to the customer should remain relatively unaffected. If, however, the service provider undergoes bankruptcy, the customer would, at some point, stop receiving the services. The customer would have to direct any actions – such as claims for services paid but not performed – against the insolvent entity in the bankruptcy proceeding.

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.

Argentine Data Protection Law No. 25,326 (the Argentine Data Protection Law) will apply to the use of cloud computing insofar as it entails the processing of personal data. The Argentine Data Protection Law, and its accompanying Decree No. 1158/01, constitute the main framework on data protection in Argentina. They are enforced by the DPA.

The Argentine Data Protection Law defines personal data as any kind of information referring to identified or identifiable individuals or legal entities. The general principle under the Argentine Data Protection Law is that any processing of personal data (including any disclosure, collection, storage, amendment and destruction) must be specifically consented to by the data subject. Such consent must be prior, given freely, based upon the information previously provided to the data subject (informed) and expressed in writing or by equivalent means, depending on each case.

Several provisions of the Argentine Data Protection Law and its complementary regulations can be relevant in connection with cloud computing. These include its provisions on cross-border data transfers, data processing agreements, and security measures and confidentiality obligations.

Regarding cross-border data transfers, the Argentine Data Protection Law prohibits the transfer of personal data from Argentina to other countries or to international organisations if the countries or organisations do not provide an adequate level of data protection, with certain exceptions. In cases when adequate data protection is not set up, transfers may still be made when the data subject consents to the transfer or when adequate protections arise from contractual clauses or self-regulated systems (as, for example, Binding Corporate Rules).

DPA Rule No. 60-E/2016 (Rule 60) provides a list of jurisdictions which the DPA considers to provide an adequate level of protection. These are the member states of the European Union and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faroe Islands, Canada (only applicable to their private sector), New Zealand, Andorra, the United Kingdom and Northern Ireland, and Uruguay. Moreover, Rule 60 approved two sets of standard model clauses addressing the two most common types of data transfers: the assignment of data to a third party and the transfer of data for the rendering of data-processing services.

In connection with data processing, any entities that provide outsourced processing services, including cloud computing entities, are considered data processors. In that case, the Argentine Data Protection Law requires a data processing agreement between data processor and data controller. Decree No. 1558/2001 provides that the agreement must:

- detail the security measures mandated by the Argentine Data Protection Law;
- include the parties' confidentiality obligations;
- establish that the data processor will only act as instructed by the data controller; and
- establish that the data processor is also bound by the Argentine Data Protection Law's data security requirements.

The data may only be used for the purpose outlined in the agreement, and may not be assigned. After the data processing has been rendered, the data must be destroyed.

Lastly, in relation to security and confidentiality, the Argentine Data Protection Law states that the data controller and the data processor must adopt the necessary technical and organisational measures to

guarantee the protection and confidentiality of the data. DPA Resolution No. 47/2018 approved two sets of recommendations in connection with security measures for the processing and conservation of personal data. One is aimed at computerised data processing, while the other is aimed at non-computerised processing. They include guidelines on measures on collection, access, modification, recovery and destruction of data, as well as on vulnerability management, security incidents and development.

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)?

As a rule, cloud computing contracts are generally non-negotiated, and customers may choose from different options. Pay-as-you-go type subscriptions, baseline agreements and PaaS subscriptions are all common. In baseline agreements, the customers are able to estimate the amount of services they expect to require, which allows them to have access to better pricing conditions than those available in pay-as-you-go models.

Overall, provisions contained in cloud services agreements are more or less standardised among different global providers, and tend not to vary greatly.

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?

In connection with governing law, some providers establish the law and courts of the country where their headquarters are located. However, providers with local presence may establish the application of Argentine law instead. Dispute resolution terms may differ, and include local courts, foreign courts or arbitration.

Choice of law and jurisdiction clauses may be subject to restrictions if Argentine law applies. For example, under the CCC, disputes arising from consumer agreements cannot be resolved by arbitration.

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?

In connection with commercial terms, providers tend to offer a range of various rates and prices for different services. Payment schemes can be either fixed or offer greater flexibility. Prices are usually set in US dollars and converted to Argentine pesos at the exchange rate applicable when issuing the invoice. Most providers allow for payment in US dollars or Argentine pesos.

Acceptable use policy terms usually list behaviours and actions that are considered unacceptable, and state that the provider reserves the right to discontinue the service if the customer engages in these activities. Regarding variations in the terms of service, providers tend to include provisions that allow them to alter the terms and conditions of the services and regulate how notification occurs.

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?

Cloud computing contracts tend to provide that the service providers will implement security measures to protect their customer's content and prevent any unauthorised access. In particular, this type of agreements may establish that only the service provider's employees or contractors will have access to the customer's content and, only as required, to render the services. Some systems may include the possibility of encrypting certain data, or of replicating data in different servers to ensure access to the content in the event of a system failure.

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?

Cloud computing services contracts generally contain clauses which limit the provider's liability. Some of these clauses limit the total liability of the provider for any claim to the amounts paid for the service. Others state that liability is limited to the farthest extent allowed by the applicable laws.

Under the CCC, any provisions that limit liability are invalid if they affect inalienable rights, are against good faith, good customs or imperative laws, or are abusive.

In relation to warranties and provision of services, it is common for agreements to include a clause that states that services are provided 'as-is'. Conversely, they tend to exclude specific warranties, such as non-interruption of services or freedom from errors. They may, however, include clauses related to a reasonable level of care or diligence.

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?

In connection with IPR ownership of content, cloud computing contracts usually state that the customers' content belongs exclusively to them, and that the agreement grants the service provider no IPR rights. Any access or use of the content by the service provider is generally restricted to that which is necessary to provide the services.

Moreover, cloud services agreements generally state that the customer is responsible for its content, and must obtain all the necessary consents and ensure that there is no infringement of third-party rights. An infringement of third-party rights could be listed as an action that violates acceptable use. In addition, there could be a limitation of liability or indemnity provision related to IPR claims filed by third parties for customer content.

Typical terms covering termination

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

Considering that, in the case of B2B cloud computing, the services provided may be important for the customer to be able to continue its ordinary business, the terms of a cloud contract may include provisions that aim to regulate the transition to another service provider or the migration of data.

Regarding termination, contracts usually state that either party may terminate the cloud services agreement due to non-compliance of

the other party. From the standpoint of the service provider, a customer infringement could include lack of payment, violation of the acceptable use provision or infringement of third-party rights. There may also be a unilateral right to terminate the contract for both parties, after a certain prior notice has been granted.

Employment law considerations

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

There are no labour or employment law considerations that specifically apply to cloud computing. As a result, general principles and provisions set forth in international treaties, the Argentine National Constitution, the Labour Contract Law No. 20,744, collective bargaining agreements, case law and any other labour regulations could be applicable.

These general principles include the employer's ability to organise the company economically and technically, and the control over the worker's activity and working conditions. A corporate policy on electronic communications and tools in the workplace could be considered among those instructions. In turn, employees' compliance with the policy could be regarded as part of the duty of due diligence and cooperation. A case-by-case analysis, though, is key to confirming this rule as applicable to specific facts.

During the past few years, labour case law has been developing an increasing broad concept of working tools, which have included not only a corporate email account, but also information technologies, computers, software, internet access and internet use, among others.

As a result, case law and most legal authors agree that corporate email and other communication tools should be deemed as work tools and, thus, the employer should be authorised to duly control its use. Nevertheless, taking into account that the situation is doubtful and has no specific legal framework, it is of high relevance that monitoring of any kind over the employee's electronic communications and devices is performed with extreme caution, as the existence of potential claims cannot be ruled out. The chances of an employer's success in the event of a claim for such unilateral email control would be higher, yet with no result guaranteed, if there is a specific policy regarding terms and conditions for use of the electronic communications and devices, duly notified to the employees in writing. This provides employees with a hard copy of the internal policy applying to the employees in Spanish, or two languages, and the employer should have them sign an acknowledgement of receipt and acceptance of its terms and conditions in wet ink signature that, among other aspects, would be convenient to expressly indicate:

- how to use email accounts provided by the company;
- that the employer is entitled to regularly check and monitor such email accounts and there shall be no expectation of privacy; and
- that any breach to the employer's policies could lead to the applicable sanctions.

TAXATION

Applicable tax rules

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

Any company performing activities in Argentina will be subject to the general tax regime. In addition, if the company complies with the requirements set forth in the Software Law (which will remain in effect until 1 December 2019) and/or the Promotion Regime of Knowledge Economy Law (which will become effective as of 1 January 2020 and will be valid until 1 December 2029) to qualify for this promotion regime, it may also benefit (see question 7).

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.

In relation to VAT, this tax applies, among other things, to the provision of services rendered within Argentina. The current general rate for this tax is 21 per cent. However, in cases where the services are rendered in Argentina but effectively used or exploited abroad, they would be deemed as rendered abroad and, therefore, would not be subject to VAT.

A recent amendment to the VAT Law introduced a new taxable event related to the provision of digital services by an individual or company domiciled abroad when its use or effective exploitation is carried out in Argentina, as long as the customer is not subject to the tax for other taxable events and does not assume the status of a registered taxpayer.

The VAT Law also includes a definition of digital services, which are understood, regardless of the device used for download, display or use, as those carried out through the internet or any adaptation or application of protocols, platforms or technology used by the internet or other networks through which equivalent services are provided that, by their nature, are basically computerised and require minimum human intervention. The tax resulting as a consequence of the provision of digital services is paid by the customer directly or through a reverse withholding mechanism.

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 EU's General Data Protection Regulation (GDPR) may have an impact on the provision of cloud computing services in Argentina, since the most important service providers are global companies. In this context, and taking into account that the GDPR has extraterritorial application in some instances, its existence may translate in practice to a higher common standard in data protection matters.

Also, as already mentioned, the regulation issued by the Argentine Central Bank in November 2017 allowing financial entities – among others – to hire from third parties those information technology services listed by the Central Bank, has been seen as a step forward in fostering cloud services in the financial sector.

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?

There are currently no draft laws that refer specifically to cloud computing.

Furthermore, in 2018, the Argentine Executive Branch introduced before Congress a bill intended to replace the Argentine Data Protection Law (the Data Protection Bill). The Data Protection Bill is generally in line with many approaches proposed by the European General Data Protection Regulation (GDPR). The Data Protection Bill includes several aspects relevant to cloud computing. Among other things, it:

- limits the concept of data subject to natural persons and excludes legal entities;
- revisits general concepts included in the current Argentine Data Protection Law, such as databases, personal data and sensitive data, and it incorporates new ones;
- includes accountability obligations and eliminates the requirement of registering databases with the DPA;
- establishes that the legal basis for the processing of personal data is still the data subject's express consent, although under specific circumstances, consent can be given implicitly, with the addition of the data processor's legitimate interest as a new legal basis;
- expressly acknowledges the right to be forgotten and the right to data portability;
- includes an obligation to notify of data breaches in certain cases;
- includes an obligation to appoint a data protection officer in public agencies, big data operations, and when the processing of sensitive data is a principal activity; and
- mandates the enactment of an impact analysis when the data processor intends to treat personal data in such a way that there is a high risk of affecting fundamental data subject rights.

Diego Fernández
dfer@marval.com

Av Leandro N Alem 882
Buenos Aires
Argentina
Tel: +54 11 4310 0100
Fax: +54 11 4310 0200
www.marval.com

Austria

Árpád Geréd
Maybach Görg Lenneis Geréd Rechtsanwälte GmbH

MARKET OVERVIEW

Kinds of transaction

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

Austria has seen a rising adoption of cloud computing applications in recent years. Although less than a decade ago the legal possibility of using cloud computing was still widely discussed, now most Austrian businesses make use of cloud computing offerings, ranging from full cloud-sourcing to single applications.

Of the various XaaS offerings, the use of infrastructure-as-a-service (IaaS) as well as software-as-a-service (SaaS) are the most prevalent. Due to the large amount of small and medium-sized businesses, cloud storage and backup solutions as well as cloud applications are statistically used most and have a very high acceptance in relation to the number of businesses. This is also due to even small IT service providers offering managed or cloud solutions, usually related to storage and backup. Those offerings are hosted either at the providers' own data centres or collocated at premises of a larger provider mostly in Austria or Germany.

The systematic and strategic use of multiple cloud offerings, up to full cloud-sourcing is usually reserved to IT- or medium to large companies in Austria. However, even there private and hybrid cloud models are prevalent.

Public authorities also make use of cloud offerings, though more from national providers rather than big international providers. In this area the former federal data centre, the BRZ, now a publicly owned private entity, is seen as the prime provider, also hosting third-party solutions for public authorities.

The most noteworthy public cloud offering is the Electronic Data Management portal, a SaaS-application that is provided by the Federal Ministry of the Environment, hosted at a publicly owned private entity and independently certified by the StarAudit (www.staraudit.org).

Active global providers

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

Almost every international cloud service provider is offering their solutions in Austria. While companies from the United States as well as Europe have been in the market almost from the very beginning, companies from Asia entered the market only relatively recently. Thus, disregarding single receptions, there is in general a west-to-east decline as far as market share is concerned.

Active local providers

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

Naming all Austrian cloud service providers would be impossible, since most of them are small to medium-sized IT service providers that also offer managed and cloud services, usually storage and backup solutions, first and foremost to their existing customers.

Among the largest local cloud providers are the former federal data centre, the BRZ, now a publicly owned private entity, as well as Fabasoft, a company that started with software solutions tailored to public authorities and is now a major local cloud provider with data centres in Austria, Germany and Switzerland.

Market size

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

According to the most recent data published by Eurostat (the statistical office of the European Union situated in Luxembourg), adoption of cloud computing solutions is increasing. While with 23 per cent it is still below the EU average of 26 per cent, it has nevertheless doubled since 2014. To put this into context: the heaviest users of cloud computing in the EU are Finnish and Swedish businesses with an adoption of 65 per cent and 57 per cent respectively.

This percentage once again varies according to the size of the business in question, with larger businesses showing a significantly higher – more than 50 per cent – adoption of cloud services than small or medium-sized ones.

Although this data is accurate in regard to major cloud services, it does not fully take into account the small local managed and cloud service offerings from, for example, IT service providers.

Of all the cloud computing offerings, storage, email and office software are the most widely used cloud solutions.

The value of the Austrian cloud computing market was around €600 million in 2018 and is estimated to increase to about €685 million until 2021.

Impact studies

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

Various studies on the use of cloud computing are publicly available and updated regularly. However, the only truly independent study is the one conducted by the Statistik Austria, the federal statistical office of Austria, the data of which is then shared with the Eurostat.

Most of the studies are conducted by stakeholders and audit companies can, therefore, not be considered truly independent. Nevertheless, they sometimes provide very detailed insight into various aspects of

cloud offering. As such, they are very often the only sources for certain, detailed statistical information.

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 Austrian government, especially the Kurz government (December 2017 to May 2019), has a strong focus on not only aiding the adoption of new technologies but also fostering the creation of such technologies and the uses for the same. The keyword used for this in Austria is 'digitalisation' and the Kurz government even denominated a federal ministry to be responsible for all such matters. Cloud computing as a basis of many modern technologies is the natural beneficiary of this policy.

With Austria's leading role in the field of e-government (ranking 6 of 34 in the 2018 eGovernment Benchmark of the European Commission), a general commitment of the federal government to pool and most efficiently use IT-resources and the above-mentioned fostering of 'digitalisation', cloud computing has been and still is on the rise in Austria, doubling the number of businesses moving to the cloud between 2014 and 2018.

Despite all this, the Austrian government has never adopted a true 'cloud first' strategy and has also refrained from obliging public entities to ask for at least one cloud offering when inviting tenders for software, IT infrastructure or IT services.

Incentives

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

While Austria does not offer any fiscal, custom or other direct monetary incentives simply for making use of cloud computing offers, Austria offers a wide range of funding programmes, many of them together with the EU, for the purpose of promoting digitalisation.

Many of the programmes are tailored to research projects, though also including projects that aim to create solutions suitable for public use. However, there are also programmes funding investment into IT in general and e-business applications. Some are exclusive to small and medium-sized businesses.

Apart from entities on the state level, the Austrian Research Promotion Agency is the main federal funding body.

LEGISLATION AND REGULATION

Recognition of concept

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

Austria has a tradition of keeping its laws as technology neutral as possible. Consequently, it has no law regulating cloud computing or any other technology. Rather, the general rules of civil law apply. Due to the nature of cloud computing and the many parties usually involved in providing a certain service, special attention is given to the rules on liability for third parties employed to fulfil a contractual obligation.

Over the years, many guidelines, such as from the EuroCloud Austria or the Austrian Chamber of Commerce, have helped to establish general recommendations and best practices but also to harmonise the general expectations relating to business-to-business cloud computing contracts.

Governing legislation

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

Austrian law does not provide any specific rules related to cloud computing. The closest any generally applicable legal provision gets to influencing the potential use of cloud offerings are the EU General Data Protection Regulation (GDPR) and the Austrian Data Protection Act (DSG), which generally prohibit the transfer of personal data to countries that do not meet the data protection standards applicable in the EU.

The only legal provision, albeit a very specific one, mentioning the use of cloud computing (though not by name) are the Guidelines for the exercise of the legal profession (RL-BA), which, in principle, merely aim to ensure and protect a lawyer's legal obligation to confidentiality. In article 40, paragraph 3, the guidelines state that any lawyer 'employing the services of an external data centre to store internal documents' needs to contractually oblige the provider to inform the authorities in case of a seizure that the data of a law office is stored and thus cannot be seized. Also, the provider needs to be contractually obliged to inform the law office in the case of any such seizure or ascertain that the data cannot be illegally seized.

The guidelines explicitly prohibit the use of any provider that does not meet these requirements, thus effectively ruling out all providers that either do not offer the required options or cannot be negotiated with to amend their contract accordingly. In practice, IT service providers providing cloud storage services, as well as other local cloud providers, usually accept the necessary safeguards so that Austrian law firms are not restricted to a few specialist providers.

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

As in every civil law country, Austria has a large number of laws governing various aspects of business or other activities. As far as cloud computing is concerned, any law providing legal rules or restrictions regarding business activities, including laws on employment relationship, is thus, in principle, able to indirectly affect and govern the use of cloud computing. This is particularly true for special legal rules relating to certain businesses, such as banks or insurance agencies.

The most prominent examples remain the GDPR and the DSG, the Austrian Data Protection Act. However, the Austrian Labour Relations Act (ArbVG) (articles 96, paragraph 3 and 96a) is another prominent legal provision with significant practical influence on the use of cloud computing and any new technology in general. According to this provision, the implementation of any technical system used to control employees requires the consent of the works council if such system affects human dignity. This also applies to the implementation of systems automatically gathering data on the employees 'that go beyond the general information and prerequisites related to the employee' as well as evaluation systems requiring the works council's consent. While consent for the latter two systems may also be obtained directly from the employees, the former rule cannot be circumvented by individual agreements between employer and employee. Rather, such 'control systems' are absolutely forbidden should no works council exist. As to which systems are actually covered by these provisions, interpretations can vary widely and usually depend on the point of view of the evaluating person. In practice, however, this has led to employers regularly informing works councils of new technologies, even if only to mention that they do not constitute any control, data gathering or evaluation system according to article 96, paragraph 3 and 96a ArbVG. In turn, works councils regularly make use of their rights to information and

consultation in such cases, thus giving them significant practical influence on decisions regarding new IT solutions in general, including cloud computing.

Breach of laws

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

As no laws specific to cloud computing exist in Austria (if one disregards the RL-BA), the consequences of a breach are always those attached to the law itself. As such, in general one can distinguish between criminal, administrative or civil consequences.

Criminal consequences are usually a result of a breach of the Austrian Penal Act. In relation to technology this is the case, for example, with hacking or identity theft. Depending on the nature and severity of the crime committed, the consequences can range from a fine to imprisonment.

Administrative consequences are usually fines due to a breach of public law. The most prominent example of one such law is the GDPR. But also breach of, for example, the Austrian Banking Act can lead to administrative proceedings and fines, in this case by the Financial Markets Authority.

Finally, civil consequences are those related to either tort or a breach of contract, which in turn need to be evaluated against the general civil legal rules. The usual consequence of such a breach is the obligation to compensate financially for any damage caused. In the case of unfair competition, publication of the verdict may be ordered in addition.

Of course, the consequences are not exclusive. Thus any breach of criminal, administrative or civil rules may additionally lead to consequences of another nature. Once again, the GDPR can serve as an example. Article 82 explicitly grants any person the right to claim compensation for damage caused by a breach of the GDPR. This right exists in addition to and independently of the national data protection authority's (DPA's) right to impose a fine upon the company in breach of the law. Thus even if the DPA would decide to abstain from a fine and merely issue a reprimand for a minor breach, any affected person may still claim compensation should the breach have caused damage.

Consumer protection measures

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

Consumer protection rules are mostly stipulated in the Austrian Consumer Protection Act (KSchG). However, for business-to-consumer contracts concluded on the internet, the rules set forth in the Austrian Act on distance and out-of-office selling (FAGG) are the most relevant and have partially been moved over from the KSchG.

In general, the FAGG stipulates very strict and detailed information obligations regarding the identity and contact details of the business, even more so than the generally applicable E-Commerce Act. In addition to requiring businesses to provide the required information to the consumer before a contract is concluded, businesses are furthermore obliged to transmit that information as well as the contractual terms to the consumer in a way that allows him or her to save all this information and documents. In practice, this is usually effected by sending a confirmation email with attachments to the consumer. In the case of a breach, the law grants the consumer a very long deadline within which to decide to withdraw from the contract without any consequences.

Even after the binding conclusion of a contract, the consumer can still decide to withdraw from the contract without giving any reason and without consequences within 14 days.

As far as digital services are concerned, however, the law provides the possibility to waive this right of withdrawal. Namely, if a service provider starts with the provision of the services upon explicit request of the consumer before expiration of the 14-day deadline, the consumer thereby waives his or her right of withdrawal. In practice, cloud service providers as well as app stores and providers of digital media require the consumer to explicitly consent to the immediate provision of services, usually by ticking a box, before expiration of the deadline. Without such consent, the providers simply do not conclude a contract with the consumer in the first place.

In the case of disputes between a business and a consumer, though not in cases of disputes between businesses, the Austrian Alternative Dispute Resolutions Act additionally applies.

Sector-specific legislation

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

With the notable exception of the RL-BA (see question 9), Austrian law does not contain specific rules relating to cloud computing. As such, sector, industry or profession-specific rules apply to and affect cloud computing insofar as they impose specific rules and requirements on third parties that the relevant regulated business or entity deals with.

In general such rules can be found, for example, in the Austrian Act on Public Tenders and associated the case law as far as rules are set forth on how to evaluate the suitability and qualification of a party providing an offer.

Other rules may be found in the banking, finance, insurance, energy or telecom sectors, where providers are regulated very strictly and care is taken that the strict obligations are not watered down by using for example for core services and obligations third parties that do not meet those strict requirements.

Insolvency laws

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

In the absence of specific legal rules on cloud computing in Austria, the general rules of the Austrian Insolvency Act (IO) apply.

Of particular note and importance to cloud computing are articles 21 and 25a IO. According to these provisions, the insolvency administrator has the right to decide whether to continue or end any contracts still in force and not completely fulfilled by the time insolvency proceedings are opened. The contracting partner of the insolvent business, however (in our case: the cloud service provider), is barred from terminating the contract, unless for a good cause, for a period of six months after opening insolvency proceedings, if such termination may endanger the continuation of the insolvent business. In practice, this means that usually no cloud provider, except for very minor and niche services, can terminate the contract and suspend provision of the services upon the opening of insolvency proceedings. Rather, they would need to ask for a declaration of the insolvency administrator as to whether he or she chooses to continue or terminate the contract.

While this provision was created with services such as electricity in mind, it nevertheless affects all other business-critical services, including cloud offerings.

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.

The most important and general rules on data protection in Austria are set forth in the GDPR and the DSG. However, specific data protection rules, for instance, relating to employment contracts, have additionally been introduced into the relevant sector, business or topic-specific acts.

All data protection rules have in common that they only govern the processing of personal data, which is data by which a natural person can be identified. Since business data always also contains personal data (for example, the names of users or contact persons), the relevant rules are also applicable if such data is stored at a cloud computing provider.

In principle, the GDPR demands personal data to be processed only based on legal grounds. Those can be, for instance, consent or the necessity to process the personal data to fulfil a contract concluded between the natural person (data subject, here the user) and the contracting partner (processor, here the cloud provider). A typical application of a necessity to process would be the processing of the user's name and address by the cloud provider for the purpose of billing.

Furthermore, the GDPR demands that any personal data shall only be processed for specific purposes. Thus in the example above the cloud provider is not allowed to use the user's contact data for marketing purposes if it was only collected for the purpose of fulfilling the contract (that is, maintaining an account with credentials, billing and any other use required by the service itself).

This configuration becomes more complex in a typical business-to-business environment, where the user is no longer the data subject, but rather a business that itself processes personal data of its own users, employees and others and is thus itself controller. The cloud provider's role is then changed to that of the 'processor': an entity that no longer processes personal data for its own use but for, and according to the instructions of, a controller. In this configuration the rules regarding the legitimate processing of personal data still apply. Thus the business user (controller) needs to ensure that it cannot just legitimately use, but can also transfer personal data to the cloud provider (processor). Additionally, the controller needs to conclude a written contract with the processor ensuring that it will process the personal data only within the scope of the contract with and instructions of the controller (see article 28 GDPR for further details). Even though the controller and processor are jointly liable according to the GDPR, the main accountability and liability nevertheless rests with the controller.

While contracts requiring cloud providers to generally follow instructions from their users regarding the data stored in their environment would have been quite unthinkable a few years back, such contracts have now become a legal requirement and thus the norm.

Apart from formalities involving written contracts, declarations and similar, the single most fundamental rule of the GDPR is that compliance requires appropriate technical and organisational measures to fulfil the obligations set forth by the GDPR and protect the personal data, where 'appropriate' depends on the sensitivity of the personal data involved. As such, healthcare data needs to be better secured against illegitimate access and use than merely some names. With this rule, the GDPR requires cloud providers but also their business users to take proper IT security measures, which never involve only a technical component, but always also an organisational one, at least in the form of raising the awareness of the employees in regard to security, personal data and compliance in general coupled with explaining why the rules are in place and need to be observed. This is, in practice, one of the bigger hurdles – less so for larger businesses, be they cloud users or cloud providers, but rather for small and sometimes even medium businesses. Before the GDPR those businesses shied away from investing the required, and not insubstantial, amounts of time and money to implement proper technical and especially organisational measures and have preferred to implement a minimum or perhaps modicum of technical security measures. With the increase in the DPA's fines for not implementing appropriate technical and organisational measures, this aspect of the GDPR becomes more important. In this regard, cloud computing providers can actually provide an added benefit for their business users by implementing just those appropriate technical and organisational measures that the user would be lacking if it was still storing the data on its own premises.

This also ties in with the duty of articles 33 and 34 GDPR to report data breaches within 72 hours and also provide certain details required by law. Without a proper IT security system in place, which includes an appropriate organisation, businesses would be hard pressed to meet those requirements.

A final very important rule of the GDPR is the requirement of the controller to ensure that data is only transferred to countries with an adequate level of data protection, consistent with the level provided by the GDPR (see articles 44 and following GDPR). This, of course, adds additional hurdles to the transfer of data to cloud providers or any of their data centres situated outside of the EU or a country with a recognised adequate level of data protection. In practice, this has, on the one hand, led many international cloud providers to store the data of their EU users only within their EU data centres. On the other hand, businesses from the EU are now more than ever looking for and preferring cloud service providers (be they IaaS, PaaS or SaaS-providers) who offer just this added benefit and legal ease of use.

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)?

Austrian law does not require contract to abide to any of the contract forms determined by law. Rather, businesses are free to combine any and all elements. Only in case of a dispute and if the contract is unclear will a court determine under which contractual form a provision in dispute needs to be interpreted. This then determines the legal consequences attached to such form. Austrian courts, however, regularly determine the form for each provision in dispute separately. Mixed contracts are common and widely accepted in Austria.

In practice, however, this poses fewer issues than one might believe. Since, especially in a business-to-business environment, the parties are free to conclude agreements that differ from the legal rules applicable in the case of a lack of an individual agreement, a detailed contractual agreement usually helps to finally determine all contractual rights and obligations and avoid a differing interpretation in the case of a dispute.

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?

In most cases, cloud providers in Austria conclude contracts based on their own standard contract templates or general terms and conditions. Notable exceptions are significantly large users and public entities, which usually have their own standard contractual templates or clauses, and tenders, where the patron usually provides the contract as part of the tender.

Since most of the international cloud providers also have companies in Austria, the governing law is usually Austrian law with the venue being the relevant court at the seat of the cloud provider. These clauses also serve to clarify any cross-border issues that may arise from either the user and the provider having their seats in different countries or the cloud service being provided in multiple countries.

Enforceability is not an issue within the EU, due to the cross-border recognition of judgments according to the Brussels I-Regulation (Regulation (EU) 1215/2012). Otherwise, the parties (usually the user) will need to evaluate and decide whether the relevant special rules regarding enforceability are simple enough to accept the jurisdiction.

This being said, not only are alternative means of dispute resolution becoming more and more common in cloud contracts, but also more cooperative approaches are seeing increased use in IT contracts in general. The aim of those is not to provide alternatives to a state court, but rather to implement determine a communication system, which helps the contracting parties to discuss and solve issues before they can escalate.

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?

Owing to the large number of providers and services, there are not clear 'typical' terms for public business contracts.

In general, most SaaS offerings are paid according to the number of users, while the price of IaaS and PaaS usually depends on the amount of data.

In general, public cloud contracts contain a minimum to modicum amount of service, which can then be expanded either in whole packages or by purchasing additional modules or services. This helps to meet a large basic demand while still offering standardised upgrade possibilities.

As a rule, public offerings tend to be more restrictive towards the user, especially regarding rights and liability rather than private offerings.

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?

Typical data protection terms are heavily regulated by the GDPR and the DSG. Therefore, cloud providers and their users have relatively little leeway in fleshing out the legal rules. In practice, most of the data provisions in cloud and other IT contracts are very similar, with small variations depending on whether the cloud provider or the user has drafted the contract.

A new trend introduced by the GDPR involves annexes with a (as the case may be more or less detailed) list of all technical and organisational measures in force at the cloud provider. While such annexes were provided from time to time before, most cloud providers preferred not to share such information for security reasons.

Confidentiality is also ensured contractually by standard clauses, for example, determining what constitutes confidential information and ensuring access only on a need-to-know basis. A new trend in this regard is slowly developing due to the transposition of the Trade Secrets Directive into Austrian law, namely articles 26a to 26j of the Austrian Act on Unfair Trade Practices (UWG). According to the now legal definition of a 'trade secret' in article 26b UWG, trade secrets not only need to be confidential and of value, but also subject to appropriate measures of protection. These include technical and organisational measures. Thus, in contrast to existing standard clauses, where parties tended to consider next to every information 'confidential' and simply demanded the recipient to implement 'at least the same level of protection', the new understanding ties in rather well with the rules of the GDPR demanding appropriate technical and organisational measures. While this does not prohibit parties from considering every type of information confidential, it at least helps to clarify which measures of protection can be deemed appropriate. In contracts containing an annex listing the technical and organisational measures taken for the purposes of data security and protection, those measures are at the same time considered appropriate for the protection of the confidential information, unless agreed otherwise.

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?

Usually, cloud providers tend to limit their general liability to gross negligence and wilful misconduct and, further to foreseeable and positive damage. This is, however, a limitation quite prevalent in business to business contracts. Another often used limitation is to further cap the liability for gross negligence with an amount tied to the value of the contract.

While liability for personal injuries cannot be limited by law, this type of liability is irrelevant for cloud computing contracts in practice.

That being said, Austrian cloud providers in particular are relatively generous where their liability for service levels (availability, reaction time, etc) is concerned, often offering penalties if the agreed service levels are either not met or not met after a certain period of time.

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?

Usually the liability regarding intellectual property rights are divided between the cloud provider and the user, depending on who provides which content. Therefore, the cloud provider usually assumes liability for any infringement caused by the cloud offering itself, while the cloud user assumes liability for infringements caused by the content it stores, alters or generates using the cloud offering. Both parties guarantee reciprocally that they each hold all necessary intellectual property rights to provide the service or store, alter or generate the content respectively.

With regard to the generated content, some SaaS contractually offerings reserve all rights regarding automatically generated content based on raw data, for example, graphics, charts or analysis', granting the user merely a right to use the thus generated content for the contractual purposes. While such provisions have not yet been challenged before court (or at least no relevant decision has been published), it is doubtful whether they would hold up before judicial scrutiny, as the generated content nevertheless also depends on the input and could, therefore, be qualified as a joint work, to which the cloud provider and cloud user jointly hold all intellectual property rights.

Typical terms covering termination

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

The termination options of cloud contracts greatly depend on the service in question.

While many public, easy to implement offerings, such as storage or SaaS solution, allow for flexible conclusion, amendment and termination of the contract, other, more complex offerings, especially private cloud solutions, provide for a minimum contract term of one or two years, much depending on any costs of implementation and expected amortisation. Almost all contracts have in common that they automatically extend rather than end after the end of the minimum contractual term.

Today most contracts not only contain detailed provisions on immediate termination for good cause, but also on procedures to allow the user to export its data from the cloud environment. This includes advance warning notifications and, in many cases, even a period of a few weeks up to a number of months after the effective end of the contract for which the cloud providers guarantee to keep copies of the data to ensure proper export and migration. Assistance for this purpose is usually subject to additional payment.

Since the entry into effect of the GDPR almost all cloud contracts also specifically state the deadline within which the user's data will finally be deleted.

Employment law considerations

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

The most relevant employment law rules relating to cloud computing are articles 96 para 3 and 96a ArbVG. These provisions require the consent of the works council for the implementation of any technical system used to control employees that affects human dignity as well systems automatically gathering data on the employees 'that go beyond the general information and prerequisites related to the employee' as well as evaluation systems. Only the consent for the latter two systems may also be obtained directly from the employees. Due to the rather broad understanding of the potentially relevant systems, employers regularly inform works councils of new technologies and works councils regularly make use of their rights to information and consultation, giving them significant practical influence on decisions regarding new IT solutions in general, including cloud computing. See question 10 for details.

TAXATION

Applicable tax rules

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

Taxation for cloud computing companies in Austria does not follow any special rules. Thus cloud companies are taxed in the same way as any business, and taxation in Austria is first determined by whether the main seat of the business is in Austria, and if not, on the offerings provided in Austria.

Servers in Austria are usually not considered sufficient legal grounds for taxation, unless they or the data stored on them represents a 'significant part of the business'. Should this test lead to the taxation of a company (be it a cloud provider or cloud user) both in the country of its main seat and those of its servers, the relevant double taxation agreements apply.

MAYBACH · GÖRG · LENNEIS
& PARTNER RECHTSANWÄLTE

Árpád Geréd
a.gered@mglp.eu

Museumstrasse 5
1070 Vienna
Austria
Tel: +43 1 997 19 66
Fax: +43 1 997 19 66 100
www.mglp.eu

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.

No special taxes apply to cloud computing offerings in Austria. Rather, such offerings are subject to the same taxes, including VAT, as any other service for which Austrian tax law does not provide specific rules.

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.

In Austria no notable cases or decisions regarding cloud computing offerings have been published.

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?

After the entry into effect of the GDPR, the currently biggest challenge cloud providers and cloud users are facing is the increased focus of the data protection authorities on accountability. Thus, where the lenient treatment of infringements in 2018 caused many companies to consider their implementation of the GDPR rules as future-proof, a sharp increase in fines in 2019 is causing a trend to re-evaluate the existing measures. Another open question is the impact of the very recent NIS Act (the Austrian transposition of the NIS Directive) on cloud offerings. While, in principle, only binding for providers of critical infrastructure, some cloud providers are nevertheless considered as such. Furthermore, decisions and recommendations on best practices are also expected to influence measures taken by providers and users alike.

Bangladesh

Sharif Bhuiyan and Maherin Khan
Dr Kamal Hossain and Associates

MARKET OVERVIEW

Kinds of transaction

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

Users in Bangladesh are able to access all kinds of cloud computing services including software-as-a-service (SaaS), infrastructure-as-a-service, platform-as-a-service (PaaS) and storage. Most users generally use global international cloud providers.

Active global providers

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

Users in Bangladesh are able to access all the global international cloud providers.

Active local providers

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

Some local companies provide cloud computing services. Their services include providing SaaS, PaaS and storage services.

Market size

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

Cloud computing is still not very established in Bangladesh. We were not able to find any reliable market statistics.

Impact studies

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

We were unable to find any reliable data or studies on the impact of cloud computing in Bangladesh.

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 government of Bangladesh is taking various steps to develop the IT sector in Bangladesh. In 2014, it was reported that the Bangladesh government is planning to move to cloud computing 'G' (government) to preserve the country's sensitive data.

According to the Information Security Policy Guidelines, all government agencies will be brought under the e-governance framework. Different government ministries or divisions, departments or agencies and their subordinate bodies have started implementing e-governance. The intention is to improve and ease the government work process and to increase the productivity of the government.

According to the 'National Information and Communication Technology Guidelines 2015', one of the action plans of the government includes creating data centres to preserve government information and central hosting of e-services.

One of the leading national daily newspapers reported in 2016 that the construction of the national data centre (National Tier IV Data Centre) will be completed by 2017. This US$154- million project is being implemented by Chinese telecom giant ZTE Corporation. ZTE started building the government-sponsored centre at the Hi-Tech Park in Kaliakoir, Gazipur. The test run of the data centre, which will preserve all sensitive data of the country, started in February 2018 (www.thedailystar.net/business/national-data-centre-be-ready-2017-1302760).

Incentives

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

The National Information and Communication Technology Guidelines 2015 envisages the establishment of software technology parks, hi-tech parks and ICT incubators. To encourage investment in this sector, the guidelines also envisage tax holiday and other incentives.

Under section 46C of the Income Tax Ordinance 1984 (ITO), certain tax exemptions are available to hi-tech parks, ICT villages or software technology zones and IT parks.

LEGISLATION AND REGULATION

Recognition of concept

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

Cloud computing is not yet expressly mentioned as a commercial, technological or operational concept in our legal system.

Governing legislation

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

There is no legislation or regulation that directly and specifically prohibits, restricts or otherwise governs cloud computing, in (onshore) or outside (offshore) Bangladesh. Bangladesh is not part of the EU and, as such, EU laws do not have any direct effect in our jurisdiction.

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

Section 35 of the Bangladesh Telecommunication Regulation Act, 2001 (the 2001 Act) sets out the circumstances under which one needs licence from the Bangladesh Telecommunication Regulatory Commission (BTRC). Section 35 of the 2001 Act, inter alia, provides as follows:

> *Requirement for licence for telecommunication, internet etc –*
> *(1) Subject to subsection (3), no person shall, without a licence:*
> *(a) install or operate a telecommunication system in Bangladesh or undertake any construction work of such system;*
> *(b) provide in Bangladesh or to any place outside Bangladesh any telecommunication service;*
> *(c) undertake any construction work for providing internet service or install or operate any apparatus for such service.*
> (Unofficial translation)

The term 'telecommunication' has been defined in section 2(11) of the 2001 Act to mean transmission and reception of any speech, sound, sign, signal, writing, visual image or any other intellectual expression by way of using electricity or electro-magnetic or electro-chemical or electro-mechanical energy through cable, pipe, radio, optical fibre or other electro-magnetic or electro-chemical or electro-mechanical or satellite communication system.

Although the aforesaid provisions may be interpreted as indirectly covering cloud computing, on contacting BTRC on a no-name basis, we were informed that cloud computing service does not require a licence under these provisions.

Bangladesh is not a part of the EU and, as such, EU laws do not have direct effect in our jurisdiction.

Breach of laws

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

Not applicable.

Consumer protection measures

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

There are no specific consumer protection measures that apply to cloud computing in Bangladesh.

Sector-specific legislation

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

There is no sector-specific legislation that applies to cloud computing transactions in Bangladesh.

Insolvency laws

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

The insolvency laws in Bangladesh do not expressly deal with bankruptcy of a cloud computing supplier. Therefore, the general bankruptcy laws would be applicable. Bankruptcy in Bangladesh is primarily governed by the Bankruptcy Act 1997. The Act makes provision for, inter alia, the order of preferential payments from the distributable assets of the bankrupt, management of distributable assets, appointment of receiver and so on.

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.

There is no specific data protection or privacy legislation applicable to cloud computing contracting or contracts. There are some sector-specific data protection laws. However, these provisions apply generally and are not limited to cloud computing contracting or contracts.

For example, under the Bank Companies Act 1991, permission from Bangladesh Bank (the central bank of Bangladesh) would be required for a banking company to remove from Bangladesh certain records or documents. Bangladesh Bank has issued various guidelines and circulars on cybersecurity and ICT security. These guidelines and circulars set out various requirements that banks and non-bank financial institutions must adhere to. The Guideline on ICT Security for Banks and Non-Bank Financial Institutions of 2015, for example, sets out the minimum requirements to which banks and non-banking financial institutions (NBFI) must adhere to (eg, the bank or NBFI, which provides payment card services, should implement adequate safeguards to protect sensitive payment card data). The banks or NBFIs are required to ensure that sensitive card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission. It also sets out detailed procedure for the security of data centres in which critical systems and data of a bank or NBFI are concentrated and housed. Banks or NBFIs are required to establish baseline standards to ensure security for operating systems, databases, network equipments and portable devices.

In the telecoms sector, operators are required to maintain confidentiality of subscriber information. The Cellular Mobile Phone Operator Regulatory and Licensing Guidelines 2011 and Regulatory and Licensing Guidelines for Establishing, Operating and Maintaining 3G Cellular Mobile Phone Services stipulate various conditions in the licences of the mobile phone operators. One such condition is subscriber confidentiality. Accounting information and user information of subscribers cannot be transferred to any person or place outside Bangladesh. Similar restrictions apply to licensees providing other telecommunication services, such as an internet protocol telephony service.

The government has also taken a number of measures to ensure cybersecurity and information security. For example, the National Cybersecurity Strategy outlines a framework for organising and prioritising efforts to manage risks to the cyberspace or critical information infrastructure. It outlines minimum-security measures that

stakeholders must abide by to claim compliance with national cybersecurity requirements.

The Information Security Policy Guidelines was issued to help government agencies formulate their own Information Security Policy to protect their information in the cyberspace (including information that is moving in the intranet or LAN or in the cloud, or simply stored in an internal database or in a PC).

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)?

There is no specific form of cloud computing contracts.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

Typical terms covering termination

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

Not applicable.

Dr. Kamal Hossain & Associates

Dctthkuvgtu'0Cfxqecvgu'0Ngi cn'Eqpuwnvcpvu

Sharif Bhuiyan
sbhuiyan@khossain.com

Maherin Khan
mkhan@khossain.com

Metropolitan Chamber Building, 2nd Floor
122-124 Motijheel C/A
Dhaka 1000
Bangladesh
Tel: +880 2 955 2946/956 4954
Fax: +880 2 956 4953
www.khossain.com

Employment law considerations

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

There are no labour or employment law considerations that apply specifically to cloud computing contracting or contracts.

TAXATION

Applicable tax rules

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

There are no specific taxation rules that apply to the establishment and operation of 'cloud computing companies'. However, under section 46C of the ITO, certain tax exemptions are available to hi-tech parks, ICT villages or software technology zone and IT parks.

Under section 46C(1) of the ITO, income, profits and gains from certain physical infrastructure facilities (including hi-tech parks, ICT villages or software technology zones and IT parks) set up in Bangladesh between 1 July 2011 and 30 June 2019 (both days inclusive) are exempted from the tax payable under the ITO for 10 years beginning with the month of commencement of commercial operation, and at the rate, specified below.

Period of exemption	Rate of exemption
For the first and second year	100 per cent of income
For the third year	80 per cent of income
For the fourth year	70 per cent of income
For the fifth year	60 per cent of income
For the sixth year	50 per cent of income
For the seventh year	40 per cent of income
For the eighth year	30 per cent of income
For the ninth year	20 per cent of income
For the tenth year	10 per cent of income

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 not expressly provided for in taxation laws. However, VAT is payable on 'information technology enabled services' (service code: S099.10), which includes digital content development and management, animation (both 2D and 3D), GIS, IT support and software maintenance services, website services, business process outsourcing, data entry, data processing, call centre, graphics design, search engine optimisation, web listing, e-commerce and online shopping, document conversion, imaging and archiving, any automated services rendered by internet or electronic network, e-procurement and e-auction.

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.

None.

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?

None.

Belgium

Edwin Jacobs, Stefan Van Camp and Bernd Fiten
Timelex

MARKET OVERVIEW

Kinds of transaction

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

With regard to public, hybrid and private cloud models: the public cloud usage in Belgian companies has grown in the period from 2012 to 2016, from 6 per cent to 12 per cent to 15 per cent in 2018 . (source: Cloudmakelaar, http://cloudmakelaar.be/2016/12/meer-dan-de-helft-van-belgische-bedrijfsvestigingen-gebruikt-cloud-applicaties). Hybrid clouds are also used, although no exact numbers are available for this specific category (https://belgiumcloud.com/2018/12/24/de-belgium-cloud-barometer-editie-2018/).

In the public sector, a notable community cloud project is the development of the G-cloud. This is a voluntary cloud service for all public sectors and services to centralise public governance in a single cloud. The G-cloud is a hybrid cloud, with the possibility of offering infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS). For the development and functioning of the G-cloud, the government uses private cloud providers, such as IBM, Microsoft and Oracle.

Of the companies that use cloud services (see question 4), the following percentages apply. Storage cloud services are the most used cloud service employed by Belgian companies (71 per cent). Next to storage services, e-mail services through the cloud are also strongly represented in the Belgian economy (71 per cent). With regard to SaaS, software tools for managing finance and accounting (41 per cent in 2018), standard office software (59 per cent in 2018), and customer relationship management (CRM) (40 per cent in 2018) are commonly used in Belgium. Regarding IaaS the most used applications are hosting services for company databases (55 per cent in 2018) https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Use_of_cloud_computing_services_in_enterprises,_2018.png), processing power for proprietary company software (31.8 per cent).

Of all e-banking and e-learning solutions, almost 94 and, respectively, 80 per cent are cloud solutions. HR solutions take third place, of which almost 40 per cent is a cloud-based solution (https://belgium-cloud.com/2018/12/24/de-belgium-cloud-barometer-editie-2018/). In HR, cloud solutions are often offered by social secretariats such as Partena, Attentia, SD Worx, Xerius and Securex.

Regarding notable cloud transactions, the Belgian bank Belfius relies on the company Genesys to provide workforce management tools, which stem from cloud-based solutions.

Another notable cloud transaction was announced in 2013. IBM signed an agreement with Belgian bank Dexia and several major financial institutions in Europe to build and manage their IT infrastructure. An IBM company called Innovative Solutions for Finance (ISFF) was designated for this, and sourcing contracts for a total value of US$1.3 billion over seven years were signed. IBM agreed to implement a cloud infrastructure to expand ISFF services into new markets and optimise its existing information technology management. In 2018, Belfius Group and IBM extended their partnership. As a result, a joint venture called PI-Square was founded. The joint venture will perform services exclusively for Belfius Group (source: https://datanews.knack.be/ict/nieuws/ibm-en-belfius-verlengen-samenwerking-tot-2023/article-normal-1002527.html).

Active global providers

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

These are:

- Microsoft (61 per cent, source: Beltug, https://www.beltug.be/event/61/6256/Microsoft_Azure_populairste_cloudprovider_in_Belgie/);
- Amazon (35 per cent);
- Google (16 per cent) (Gmail, Google Drive, Google Docs, Google+, search engine);
- HP;
- IBM;
- LaCie;
- NetApp;
- Oracle;
- Salesforce; and
- Zenith.

Active local providers

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

- Acerta (SaaS for payroll and other HR services);
- Adc Antwerp (tier 3 data centre);
- ADMB (SaaS for payroll and other HR services);
- Amplidata (storage facilities);
- Arxus (hosting services);
- Attentia (SaaS for payroll and other HR services);
- Calligo (IaaS, SaaS, PaaS);
- Combell (hosting services);
- CRM-Warehouse (cloud integrators);
- First Served (hosting services);
- Groep S (SaaS, PaaS for payroll and other HR services);
- Impro Biz (implementation of salesforce CRM);
- Informat (SaaS for school administration);
- Isabel (SaaS for e-banking);
- LCL (tier 3 data centre);
- Nucleus (cloud hosting services);
- Partena (SaaS for payroll and other HR services);

- Protime (SaaS for workforce management);
- Proximus (XaaS private, public or hybrid cloud services);
- SAAS45 Channel (SaaS);
- SaaSForce (cloud services distributor – SaaS);
- SAP (PaaS for app development);
- SD Worx (SaaS for payroll and other HR services);
- Securex (SaaS for payroll and other HR services);
- Systemat (local cloud integrator);
- Telenet (PaaS);
- UnifiedPost (Saas);
- Xaop (system integration in the cloud);
- ZapFi (OTT Wi-Fi cloud platform); and
- Cloudmakelaar (http://cloudmakelaar.be/wp-content/uploads/2017/12/CSP-catalog-2017_v2.pdf).

Market size

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

We have found that the figures on the adoption rate of cloud computing services vary depending on the source. Possible reasons for this are that it is not always clear what exactly is defined as a cloud solution and how the figures were collected and analysed.

With regard to professional cloud computing use, 40.2 per cent of the enterprises in Belgium used cloud computing services in 2018 according to Eurostat (source: Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Types_of_cloud_computing:_public_and_private_cloud). This figure has been rising for a number of years now and it is significantly higher than the European Union average of 26.2 per cent.

According to the FPS Economy, the use of cloud computing services varies strongly in Belgium depending on the size of the enterprise: 76 per cent of larger companies (ie, 250 employees or more) use cloud computing services in Belgium, while only 49 per cent of smaller companies (ie, 10 to 249 employees) use cloud computing services (source: FPS Economy, https://economie.fgov.be/nl/themas/online/telecommunicatie/cloudcomputing).

Belgium Cloud is an independent group of Belgian entrepreneurs that brings together ICT experts to share and exchange information and expertise about the cloud and cloud computing. This group of experts is housed at Beltug. According to their research, there seemed to be a stagnation in the use of SaaS in 2014 and 2016, but an increase was again noted in 2018. According to their most recent report, 64 per cent of corporate establishments in Belgium use cloud applications (source: Belgium Cloud, https://belgiumcloud.com/2018/12/24/de-belgium-cloud-barometer-editie-2018/). In 2010, the adoption rate of cloud solutions in Belgium was a mere 13 per cent.

Furthermore, the use of cloud computing differs greatly from region to region in Belgium. A 2015 report by cloud service provider Aspex shows that the familiarity rate of SMEs with the cloud is high in Brussels (with 53 per cent of respondents claiming familiarity with cloud computing) while Flanders and Wallonia have low familiarity rates of 20 per cent and 26 per cent, respectively (source: Aspex, http://blog.aspex.be/nl/zijn-er-nog-belgen-in-de-cloud). These figures have also increased according to a 2017 study conducted by Computer Profile. This study shows that cloud penetration in the Flanders region totalled 72 per cent, followed by the Brussels region with 58 per cent. Lastly, the Wallonia region only counts a penetration rate of 44 per cent (source: Belgium Cloud, https://belgiumcloud.com/2018/12/24/de-belgium-cloud-barometer-editie-2018/).

With regard to individual cloud computing use, a study of the information society in Belgium has been conducted. This research shows that, of all Belgian individuals that have used the internet over the past three months, 38 per cent have used cloud storage facilities for private purposes (in 2018) (source: FPS Economy, https://economie.fgov.be/nl/themas/online/telecommunicatie/cloudcomputing). This percentage does not differ much from the years before according to the same source. It is also close to the European average of 37 per cent. If we look at the difference between men and women, we see a small difference. Men make slightly more use of cloud storage facilities for private purposes than women. It is not entirely clear what the reason for this difference is.

Impact studies

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

Cloud computing communities such as Belgium Cloud bring out reports about the state of cloud computing in Belgium from time to time. The Belgium Cloud community has published several studies on the impact of cloud computing in Belgium – for example, the 'Belgium Cloud Barometer – Editie 2018' (https://belgiumcloud.com/2018/12/24/de-belgium-cloud-barometer-editie-2018/). Also, there are other studies or barometers conducted by non-governmental actors such as Computer Profile and Cloudmakelaar ('Dit is de toestand van de Cloud anno 2018 in België' (https://cloudmakelaar.be/2018/03/dit-is-de-toestand-van-de-cloud-anno-2018-in-belgie/) or IT companies such as Christiaens.

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?

Yes, through the creation of, among others, Digital Belgium. This action plan establishes a long-term vision for the digital economy in Belgium and aims to place Belgium in the top three of the European Digital Economy and Society Index by 2020. Additional goals are the creation of 1,000 new enterprises and 50,000 new jobs across all sectors, also by 2020 (source: Digital Belgium, http://digitalbelgium.be/en).

Wallonia attempts to attract big players such as Microsoft and Google through attractive research grants and further investigation into subsidising (done by AWEX). As a consequence, Google built its first data centre outside of the US in Mons (Wallonia) in 2015 (source: Wallonia, www.wallonia.be/en/news/google-inaugurates-second-data-center-mons). In 2018, NRB Group's new data centre in Villers-le-Bouillet, a new shared data centre established by a joint venture between NRB and Etix Everywhere, was put into operation. The project offers more and secure computing space to increase the capabilities of NRB's hybrid cloud strategy (source: NRB, https://www.nrb.be/en/about/news/inauguration-belgiumdc-nrb-s-new-data-centre-minister-p-y-jeholet).

In the public sector, a notable government initiative is the community cloud project 'G-cloud'. This is a voluntary cloud service for all public sectors and services to centralise public governance in a single cloud. The G-cloud is a hybrid cloud, with the possibility of offering IaaS, PaaS and SaaS. For the development and functioning of the G-cloud, the government uses private cloud providers, such as IBM, Microsoft and Oracle (source: G-Cloud, www.gcloud.belgium.be/nl/index.html). The Belgian eHealth platform (see also question 13) makes use of the G-cloud API Gateway as transaction platform (source: https://www.gcloud.belgium.be/nl/downloads/asset/b56a4c30fcc00e16969b-bad3ce87c87eb8d4891e/eHP%20temoignageGcloud_nl_290618.pdf/application%252Fpdf). The eHealth platform is a Belgian federal government institution that offers an electronic platform where all parties

involved in public health (healthcare providers, institutions, health insurance funds, patients) can exchange information, including personal data, in a secure and efficient manner.

Incentives

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

The Microsoft Innovation Centre (MIC) Flanders aims to stimulate the development of Information and Communication Technology in the Flanders region. One of their programs is a Microsoft Azure Developer Camp. Here, companies can discover the possibilities of developing an app in the cloud through Microsoft Azure with the goal of improving, strengthening or changing their corporate projects and methods (source: Microsoft, https://mva.microsoft.com/en-US/training-courses/transforming-it-infrastructure-services-with-azure-at-microsoft-18474?l=PqWWJPMVF_1612263987).

Also, Flanders offers some fiscal incentives that promote cloud computing activities by both Belgian and foreign companies, such as a deduction of innovation income up to 85 per cent, an investment deduction for R&D projects and an exemption of payment of 80 per cent of the personal income withholding tax of researchers in certain scientific fields (source: Flanders, https://www.flandersinvestmentandtrade.com/invest/en/sectors/digital-society/cloud-computing).

LEGISLATION AND REGULATION

Recognition of concept

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

Yes, since the transposition of the NIS Directive (see below). Also, reference should be made to contract law, to specific rules on data protection (see question 15) and to the system of liability of data storage service providers (see question 10).

Governing legislation

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

Yes, the European Directive (EU) 2016/1148 on security of network and information systems (the NIS Directive) defines the notion of 'cloud computing service' for the first time. Pursuant to article 4(19) of the NIS Directive, a cloud computing service is a digital service that enables access to a scalable and elastic pool of shareable computing resources.

The NIS Directive was adopted by the European Parliament on 6 July 2016, and has been transposed into Belgian legislation. Consequently, the Belgian Law of 7 April 2019 does mention and define cloud computing services (source: E-Justice, www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&caller=summary&pub_date=19-05-03&numac=2019011507). Providers of cloud computing services (granting access to a scalable and elastic pool of scalable computer capacity) that process personal data are obliged to appoint a data protection officer.

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

In addition to the previous question, there is also Belgian legislation applicable to cloud computing services that may indirectly prohibit, restrict or otherwise govern cloud computing services.

This kind of legislation includes, first of all, legislation on data protection, such as the European General Data Protection Regulation (GDPR) which is directly applicable since 25 May 2018. A cloud provider will typically act as a processor of personal data, which means that a data processing agreement has to be concluded.

Also, legislation on outsourcing in the financial sector in the Law of 11 March 2018 (replacing the Law of 21 December 2009) on the statute and supervision of payment institutions and the institutions for electronic currencies, the access to the company of the payment services provider and the activity of issuance of electronic money and the access to payment systems, may affect cloud computing services. In this regard, cloud computing services are subject to the same principles as traditional outsourcing in the financial sector. However, cloud computing is not directly addressed by the Law of 11 March 2018, but the National Bank of Belgium (NBB) stated in its communication of 9 October 2012 that cloud computing is considered as a type of outsourcing.

The same communication of the NBB states that the circulars dealing with outsourcing, which establish rules on good practices, will remain applicable. Subsequently, the communication states that, in principle, there is no prior authorisation by the NBB required for outsourcing (in contrast to De Nederlandsche Bank in the Netherlands: see www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-februari-2015/dnb319119.jsp). Nevertheless, the NBB emphasises that it should be informed in advance on how these rules on good practices will be applied in practice (see circular PPB 2004/5 on healthy management practices in outsourcing by credit institutions and investment companies, issued by the Belgian Banking, Finance and Insurance Commission on 22 June 2004, available at www.nbb.be/doc/cp/nl/ki/circ/pdf/ppb_2004_5_circular.pdf, and circular PPB 2006/1 CPA on healthy management practices in outsourcing by insurance companies, issued by the Belgian Banking, Finance and Insurance Commission on 6 February 2006, available at www.nbb.be/doc/cp/nl/vo/circ/pdf/ppb_2006_1_cpa_circular.pdf). Recently, the NBB has issued a new circular (NBB_2019_19) implementing the guidelines issued by the European Banking Authority (EBA) on outsourcing. These guidelines will apply from 30 September 2019 and clarify the NBB's approach with regard to less significant institutions, non-EEA branches, payment and electronic money institutions. From 31 December 2021, when this circular becomes applicable to all outsourcing agreements, circulars PPB_2004/5 and NBB_2018_20, communication NBB_2012_11 and the CBFA communication of 5 November 2007 will no longer be applicable.

The Belgian Civil Code contains provisions on service contracts (article 1779 ff). These provisions may be relevant for cloud computing services. Other relevant legislation is to be found in the Belgian Code of Economic Law, which contains provisions on distance contracts (Book VI and Book XIV) and information society services, which also contains provisions on the liability of data storage service providers (Book XII), as well as new provisions introduced by the Law of 4 April 2019 in Book VI of this Code concerning unfair clauses in a B2B relationship that may create an imbalance between the rights and obligations of contracting parties and the abuse of a dependency between the parties. The latter law may have an impact on liability clauses and clauses concerning unilateral modification of contracts that are common in cloud computing contracts.

Article XII.19 of the Code of Economic Law states that where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider

is not liable for the information stored at the request of a recipient of the service, on the condition that the provider does not have actual knowledge of illegal activity or information and, as regards damage claims, is not aware of facts or circumstances from which the illegal activity or information is apparent; or the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, provided that he or she immediately communicates this to the Public Prosecutor.

Additionally, criminal law provisions in the Belgian Criminal Code and the Code of Criminal Proceedings may also indirectly prohibit, restrict or otherwise govern cloud computing services in Belgium. This includes, for example, a provision on the search in computer systems which can be extended to a computer system or a part thereof that is located in another place other than the place where the search takes place (article 39-bis, article 88-ter and 88-quater).

It should also be noted that other Belgian legislation may, whether or not implicitly, require that certain data remains within the jurisdiction of Belgium, such as article 14 of the Law of 8 August 1983 establishing a National Register of natural persons. However, with regard to the free flow of data across member states within the European Union, the legality or applicability of this kind of data localisation legislation may be uncertain in the future.

Other legislation worth mentioning is the Belgian Income Tax Code (article 315) and the Law of 13 June 2005 on electronic communications, which contains provisions i.a. on the principles applicable to the confidentiality of communications.

In the health sector, the Coordinated law of 10 July 2008 on hospitals and other care facilities was amended in such a way that it does not anymore indirectly prohibit the use of cloud computing services by hospitals. Article 20 section 1 of the Coordinated law of 10 July 2008 now states that the patient file must be kept 'by' the hospital, and no longer 'in' the hospital. After that, the FPS Public Health has drafted guidelines on this matter which were approved by the Belgian Privacy Commission (now called the Belgian Data Protection Authority) in Opinion 04/2015 of 25 February 2015 (available at www.privacycommission.be/sites/privacycommission/files/documents/advies_04_2015.pdf).

The Belgian eIDAS law, implementing the eIDAS Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, may also have indirect consequences for cloud computing in Belgium. It governs, in particular, electronic archiving, which can be very relevant for cloud computing, but it contains also rules on electronic registered mail, electronic seals, electronic signatures, websites authentication, trust service providers and electronic identification schemes.

It should also be noted that the Belgian Data Protection Authority mentions on its website that the Authority is preparing two documents on cloud computing: an opinion on 'the risks and deployment of unfolding the cloud strategy at the level of public services, including the Federal Police and Defence' and a recommendation on cloud computing targeting companies. The public sector opinion will enable public authorities to make an informed decision about how to use cloud computing to perform their tasks. The private sector opinion will include legal guidelines, as well as information security guidelines. Among other things, the issue of server locations will be discussed. In addition, the Authority will determine who is responsible for processing for each stage where data is placed 'in the cloud' (source: Belgian Data Protection Authority, https://www.gegevensbeschermingsautoriteit.be/cloud-computing). Since these opinions are not yet available, it is not yet clear whether this will indirectly restrict cloud computing services in Belgium.

Breach of laws

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

The consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing depend on the law that was infringed.

The GDPR contains some penal provisions in articles 83-84 meaning that member states should give data protection authorities, such as the Belgian Data Protection Authority (replacing the Belgian Privacy Commission), the competence to impose administrative fines on non-compliant companies. If the organisation falls within the scope of the Belgian Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data, the administrative sanctions and criminal sanctions provided for in that Act are also possible (articles 221–230).

In the financial sector, payment institutions are subject to supervision by the NBB, and the NBB may, in certain cases, withdraw the licence of a payment institution. That could be the case with the violation of circulars about outsourcing.

Regarding distance contracts and information society services, it is worth mentioning that the Belgian Code of Economic Law contains a Book XV on legal enforcement. Unfair clauses or clauses based on abuse of an economic dependency, in B2B or B2C relationships, may be declared null and void. However, in a B2B context there is new legislation that has not been applied yet by courts and it is unclear which course will be followed by case law.

Consumer protection measures

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

As regards consumer protection measures applicable to B2C cloud computing services in Belgium, it should be noted that cloud computing contracts are generally concluded over the internet, which means that those contracts are distance contracts.

The European Directive 2011/83/EU on consumer rights (the Consumer Rights Directive) establishes rules on distance selling, which is transposed into Belgian legislation. The transposition of the provisions of the Capital Requirements Directive can be found in Book VI of the Belgian Code of Economic Law. These provisions may also be applicable to cloud contracts. Consequently, in some cases, the right of withdrawal for 14 days may have to be taken into account for the conclusion of certain cloud computing contracts. However, in some cases, the right of withdrawal related to service contracts may be excluded (article VI.53 Code of Economic Law).

The European Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I-bis) implies that a consumer may bring proceedings against the cloud service provider (CSP) to a contract either in the courts of the member state in which the CSP is domiciled or, regardless of the domicile of the CSP, in the courts for the place where the consumer is domiciled. The Belgian Code of International Private Law of 16 July 2004 is in accordance with the Brussels I-bis Regulation.

Pursuant to the European Regulation (EC) 593/2008 on the law applicable to contractual obligations (Rome I), a B2C cloud computing contract will be governed by the law of the country where the consumer has his or her habitual residence, provided that the CSP pursues his or her commercial or professional activities in the country where the consumer has his or her habitual residence, or by any means, directs such activities to that country or to several countries including that country, and the cloud computing contract falls within the scope of such activities.

Sector-specific legislation

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

In the public sector, the Law of 21 August 2008 established the eHealth platform in Belgium. One of the tasks assigned to the eHealth platform is to check whether software packages for managing electronic patient files comply with the established ICT-related functional and technical standards, specifications, and to identify these software packages. Cloud service providers have to comply with certain requirements, such as security and privacy standards.

In Opinion 04/2015 of 25 February 2015, the Belgian Privacy Commission also stated that the choice for a community or private cloud does not necessarily provide more safeguards than a public cloud in terms of a better protection of personal data. Regardless of the type of cloud, the focus should be on effective data protection safeguards, according to the Privacy Commission.

In the financial sector, the implementation of the European Directive 2014/65/EU on markets in financial instruments (the MiFiD Directive) has led to some operational requirements with respect to investment firms and regulated markets, which also affect their ability to employ subcontracting or outsourcing services, including for ICT services such as cloud computing (see above).

Insolvency laws

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

On 1 May 2018, new insolvency legislation entered into force in Belgium. A new Book XX was added to the Belgian Code of Economic Law. A CSP can be declared bankrupt by the commercial court if three conditions are met, namely: the CSP is engaged in commercial activities, the CSP has suspended payments to its creditors, and is no longer creditworthy, and so the CSP will continue not to meet its obligations to creditors. If those three conditions are met, the CSP will formally be declared bankrupt by a bankruptcy judgment of the business court.

With regard to the fate of contracts concluded before the date of the bankruptcy (which are not terminated by the judgment declaring the bankruptcy), Book XX article 139 provides that the insolvency administrator may terminate those contracts unilaterally when the management of the estate necessarily requires this and that such a decision may not affect the rights in rem of third parties against the estate. The contracts are not automatically terminated unless a termination clause explicitly states so.

The bankruptcy judgment is published in the Belgian State Gazette, as well as in two regional papers. The judgment appoints the insolvency administrator (the receiver), who will perform his or her duties under the general supervision of a supervisory judge, and the judgment also provides the term for creditors to declare their claims to the insolvency administrator and the court (with a maximum period of 30 days). This declaration is necessary for all creditors who wish to assert claims against the CSP.

Subsequently, the insolvency administrator has to decide in due time whether to continue performing the valid cloud computing contracts. The customer can demand the insolvency administrator to decide on whether to perform the contract, and if the insolvency administrator does not decide within 15 days from the date of that demand, the cloud computing contract is considered terminated.

It is also worth mentioning that there is a ranking of the claims that are duly declared. All estate debts and creditors having the benefit of security interest and privileges will be satisfied first. Then the remaining assets of the CSP will be distributed by the insolvency administrator among the unsecured creditors, who rank pari passu.

The termination of the bankruptcy procedure can only be ordered by the court at the request of the insolvency administrator.

Traditionally, source code escrow agreements are used to protect software licensees against the bankruptcy of licensors. It is generally considered, however, that this practice is less interesting in the framework of SaaS contracts. In some circumstances, it can still be helpful to obtain the source code, if it is possible to deploy the software on a different system than the system provided by the SaaS CSP. In such a case, it is possible that stored data must be migrated as well.

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.

The Belgian Privacy Act of 8 December 1992 (as subsequently amended and further implemented by the Royal Decree of 13 February 2001), which was the transposition into national law of the European Data Protection Directive 95/46/EC is replaced by the Belgian Data Protection Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data (http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl?N=&=&sql=(text+contains+(%27%27))&rech=1&language=nl&tri=dd+AS+RANK&numero=1&table_name=wet&cn=1992120832&caller=image_a1&fromtab=wet&la=N&pdf_page=10&pdf_file=http://www.ejustice.just.fgov.be/mopdf/2018/09/05_1.pdf). The main source of privacy legislation applicable to cloud computing services in Belgium is the GDPR supplemented by the Belgian Data Protection Act. Other EU instruments may also have an impact, such as the European Directive 2002/21/EC (Framework Directive) and Directive 2002/58/EC (ePrivacy Directive).

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)?

Cloud computing contracts can be focused on the processing of data residing in the cloud, or can be regarded as contracts of the SaaS category, involving the online operation of applications of all kind, including more and more business-critical applications such as enterprise resource planning programmes and supply chain and logistics management, asset management and asset maintenance, workflow management, human resources, CRM, among others.

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?

B2B public cloud computing contracts are often made by international service providers, who include governing law and jurisdiction of their home state, or may include international arbitration. Belgian service providers often include an arbitration clause indicating specialized Belgian arbitration forums as competent for claims. Some contracts contain dispute resolution clauses that set forth an escalation of disputes up to the level of the executive board of the parties, and if this does not result in a positive outcome, then arbitration, court procedures, or mediation by an external third person are possibilities. With respect to enforceability, salvation clauses normally foresee that clauses that

would be invalid or unenforceable, will be automatically adapted in a way that remains as close as possible to the intended meaning of the relevant clause.

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?

If implementation services are involved, a separate price is foreseen for the implementation service, and this will be paid according to milestones, where the acceptance of the delivered service will oblige the customer to pay the relevant price. The operational cloud service is typically paid as a subscription, with annual, trimestral or monthly payments, typically paid up front. The price can be based on the allowed number of users or the used volume or number of transactions. The cloud contracts normally include an acceptable use policy, providing suspension and possibly even termination of the contract if the use policy is not respected.

Because the cloud service is often a one-to-many relationship, the service provider is practically obliged to include a variation clause in the contract, enabling him or her to modify the service unilaterally when this is needed to provide an acceptable service. To balance the rights of the customer, such clause will provide a termination right of the customer with an acceptable notice period if he or she does not agree, especially when the cost of the service is increased or certain functionalities are lost. New legislation concerning abusive clauses in a B2B context may have an impact on such variation clauses (see above).

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?

Cloud contracts will contain a description of the data centre, the communication lines and the security provisions protecting the communication and safety of the data. Data are usually located in a data centre provided by the service provider or by one of his or her suppliers. Customers that are well aware of the risks will ask for service levels that are included in a service-level agreement (SLA) with clear levels and financial sanctions (credits). Regarding data security, the service provider will usually provide encryption and access management, authorisation methods; more and more the compliance with industry standards is demonstrated through certificates.

When personal data is involved, the requirements will at least allow compliance with the legal and sectoral standards for data protection. In that case, customers require a warranty that data remain located in servers in the EU territory. If data must be transferred to, or used from, third countries such as the US, the European compliance measures must be respected. Before the GDPR, clauses regarding the notification of data breaches were not very common, but this has changed since the GDPR. General awareness about the risk of breaches on privacy has increased.

The ownership of business data is often specified in a contract, and may have an impact on the possibilities of a SaaS provider to make use of business data of customers (eg, for statistical use or for service improvement). Depending on the concrete circumstances, a customer may seek to limit such right (eg, if he or she believes that the business data could be abused or could be used in a competitive context). Similarly, the right to obtain the data after the termination of the contract is a critical issue and should be warranted by contract, whether or not at a cost price, and whether or not through migration obligations that must be executed by the cloud service provider.

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?

Every cloud contract contains some kind of limitation of liability for any damage caused by the service; liability for consequential and other indirect damages are usually excluded and direct damages are usually limited (often referring to the fee paid for the service as the limitation for damage in the aggregate).

Damage caused by intentional fault or fraud cannot be limited nor excluded by law. Although the possible liabilities of the customer are often considered as less likely, many contracts will balance the customer's liability in a similar way. Indemnities are usually provided as a safe harmless clause when a customer is confronted with a claim of a third party for infringement of its intellectual property rights. The customer can be liable for infringement on third party's rights based on infringing applications provided by the service provider, and in that case the service provider will take control of legal proceedings or negotiations and will not hold the customer liable for damages.

In the direct relationship between a data controller and his or her customer, liability for breach of the data protection rules cannot be limited. Similarly, when the customer has a direct claim against a data processor (eg, the CSP) based on a breach of these rules, his or her liability cannot be limited. It is, however, accepted that between a data controller and his or her CSP (acting as data processor), the liability can be limited even for damage caused by breach of the data protection rules.

SLAs are becoming a normal standard of cloud contracts, guaranteeing the availability of the service, timely response of a helpdesk and performance levels. The levels can be negotiated by the customer unless the service is standard for many customers: in which case, the SLA is a take-it or leave-it matter. SLAs are not always sanctioned by financial penalties; however, financial service credits are increasingly applied when the service levels are not met by the provider.

A normal cloud contract should contain clear explanation and warranties regarding business continuity and disaster recovery (eg, through replication of data or applications to spare servers); specific key performance indicators can be set forth to cover maximum loss of data packages and the time needed to be up again after a shutdown. Damages for loss of data are often excluded as damage compensation.

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?

The intellectual property rights of the applications involved in SaaS agreements or similar contracts remain with the provider of the cloud service; this is usually the case for developed interfaces and specific adaptations as well. Data and other content that is created by the customer usually belongs to the customer. The service provider's right to use such data for statistical purposes or for service improvement, or for other uses, are more and more explicitly safeguarded or, inversely, limited. Most contracts contain a provision that warrants the return of data during the course of, or after the termination of, a cloud contract.

When the cloud service is endangered because of infringement of third-party rights by the applications of the service provider, the contract clauses usually state that the service provider has the right to apply the appropriate remedy chosen by him or her, such as the adaptation or replacement of infringing code, and if that is not feasible, the termination of the contract with a partial refund of any upfront payment of fees. Damage compensation is usually excluded or at least limited.

Typical terms covering termination

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

B2B cloud computing contracts usually have a rather short applicability period (typically of one year, automatically renewable unless terminated by either party before the anniversary date of the contract). If an important investment was involved, such a contract can be agreed for three years, but usually not longer.

Termination for no cause will always take a notice period into consideration that is sufficient for both parties to find an alternative contract partner. Termination for cause, on the other hand, is foreseen in the case of material breach, usually after a grace period of one month, and in cases of bankruptcy and insolvency procedures.

The retention and return of data is of utmost importance in case of termination and is usually foreseen, although any assistance with data migration can be subject to an additional payment. The service provider will usually not provide a retention right for himself or herself, unless in case of non-payment of service fees where it might be used as a pressure mechanism

Employment law considerations

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

In some cases, outsourcing of a company's IT department may be seen as the transition of a corporate entity. In that case, the provisions of collective labour agreement No. 32-bis could be applicable (available at www.cnt-nar.be/CAO-COORD/cao-032-bis.pdf).

TAXATION

Applicable tax rules

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

There are no specific fiscal rules that apply to the establishment and operation of cloud computing companies in Belgium. Instead, the same taxation regime as for other digital service providers – and indeed, for companies in general – is maintained. Important in the context of cloud computing, however, is that these rules may require that data is held at all times within the jurisdiction of Belgium. Two separate regimes must be differentiated.

Article 60 of the VAT Code discusses record-keeping concerning invoices and equivalent documents (such as credit notes) for any taxpayer (meaning both natural and legal persons). Documents can be stored wherever the taxpayer wishes, yet they must be made available whenever the tax administration so requests. If the storage does not guarantee complete and online access, then mandatorily the invoices must be stored in Belgium. At all times, and regardless of the format, the authenticity, integrity and legibility of the invoices must be ensured.

Article 315 of the Income Tax Code also applies to all taxpayers and determines that accounting books and support documents of accounting entries must be kept on record if they can help determine the amount of taxable income. They must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent. Subject to an exception that may be granted, the books and records may be kept in another place, provided that immediate access to the books and records can be granted or that such documents can be provided on short notice in case of unannounced control. The taxation rules have been amended over the years, in particular by the Programme Law of 1 July 2016. The words 'computer system' have been replaced by 'any other electronic device' and some of the obligations have been made to apply even if the data is stored abroad. The intention was to extend the scope to cloud solutions (source: https://www.iba-boekhouding.be/wp-content/uploads/2019/06/de-fiscus-op-bezoek_0.pdf).

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.

The VAT imposed on cloud computing services follows the standard Belgian tariff of 21 per cent for goods and services that do not fall under the exhaustively determined categories of goods and services which have a reduced tariff of 12 per cent or 6 per cent. Cloud computing services also do not fall within the limited category of goods and services that are exempted from VAT. More information on the place of the provision of electronic services to persons who are not liable to VAT can be found here: https://financien.belgium.be/sites/default/files/downloads/electronic-services-en.pdf.

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.

Announced in 2013 – but still ongoing – is the already mentioned IBM agreement with several major European financial institutions to build and manage their IT infrastructure through ISFF, which was designated for this (see question 1). The total value of the deal amounts to US$1.3 billion over seven years. IBM will set up a cloud infrastructure so that ISFF can expand services into new markets and optimise its information technology management. In April 2018, IBM and Belfius announced a multi-million euro extension of their existing technology services agreement until the end of 2023.

Arguably the most important and notable case of cloud computing within Belgium was the establishment of the G-cloud. As noted before, this is a community cloud project initiated by the government. G-cloud is a voluntary cloud service for all public sectors and services to centralise public governance in a single cloud. Furthermore, it is a hybrid cloud, with the possibility of offering IaaS, PaaS and SaaS. For the development and functioning, the government uses private cloud providers such as IBM, Microsoft and Oracle (source: G-cloud, www.gcloud.belgium.be/nl/index.html).

NRB, the third-largest ICT service provider in Belgium, signed an agreement with IBM. NRB's Intelligence self-service platform works as a 'cloud broker,' which advises the customer about the managing and processing of his or her data, either in a private cloud, a public cloud or a combination of the two (source: https://www.nrb.be/nl/over/nieuws/nrb-maakt-sprong-naar-grensverleggend-cloud-computing-dankzij-partnerschap-met-ibm).

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?

The Belgian law of 7 April 2019 that implements the NIS directive is a recent framework law that still needs concrete secondary legislation specifying the obligations of the organisations targeted by this legislation. Cloud service providers can be seriously impacted by the requirements, even if the cloud service is provided on a limited scale. For example, under the current wording of the law cloud service providers are required to appoint data protection officers if they process personal data, even if the service is very limited. Furthermore, the EU Cybersecurity Act (Regulation 2019/881 of 17 April 2019), providing a cybersecurity certification framework for IT services, will have an impact that must be closely monitored.

The recent law of 4 April 2019 on unfair clauses and abuse of an economic dependency in B2B relationships may result in the invalidity of some typical clauses currently found in cloud computing contracts (eg, concerning limitation of liability and unilateral variations of the contract). It will be necessary to follow up on case law that will apply the legislation in a more or less rigorous or realistic manner.

TIMELEX

Edwin Jacobs
edwin.jacobs@timelex.eu

Stefan Van Camp
stefan.vancamp@timelex.eu

Bernd Fiten
bernd.fiten@timelex.eu

Joseph Stevensstraat 7
1000 Brussels
Belgium
Tel: 0032 2 893 20 95
Fax: 0032 2 893 22 98
www.timelex.eu/en

Brazil

José Mauro Decoussau Machado, Ana Carpinetti and Gustavo Gonçalves Ferrer
Pinheiro Neto Advogados

MARKET OVERVIEW

Kinds of transaction

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

Cloud computing is a reality in Brazil in various industry sectors and businesses. Cloud computing services and business models include the offering of cloud-based storage solutions, software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), cloud-related consultancy and other services, and both the private sector and public entities take part in contracting cloud-based solutions.

According to a 2018 research developed by Logicalis (www.la.logicalis.com/globalassets/latin-america/advisors/pt/_it_snapshot_2018_web.pdf), the private cloud model was adopted by 60 per cent of companies, while 53 per cent used the public model and 31 per cent used a hybrid solution. Hybrid solutions were expected to reach 64 per cent by the end of 2018.

Active global providers

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

The most relevant worldwide cloud service providers already have local presence or operations aimed at Brazilian customers including, for example, Microsoft, Oracle, Verizon, SAP, IBM, Google, AWS and Capgemini.

Some international providers offer cloud-based products or licences to Brazilian customers or companies through local subsidiaries or partners. Local entities are used by major international providers for marketing purposes or for maintenance and implementation, while the cloud products or licences are actually provided by foreign entities of the same economic group.

Apple and telecommunications companies, such as Vivo and Claro, also provide cloud storage services in a business-to-consumer model.

Active local providers

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

Apart from the local entities of international groups, the number of Brazilian cloud providers is increasing each year. These companies include Locaweb, Cloud2Go, Tivit, Mandic, Primesys (owned by Embratel/Claro, a telecommunications company currently owned by the Mexican company América Móvil), Uol Diveo, Binario Cloud, BRCloud, Globalweb, which offer cloud-based services, consultancy services and some of which use their partners' servers to provide services. In January 2019, Primesys/Embratel won a public bidding to provide cloud-related services to several entities of the government (including certain ministries, agencies, institutes and others), and was awarded a 29.9 million reais contract.

Telecommunications companies, such as Vivo (controlled by the Spanish group Telefónica), also provide storage services to their customers.

Market size

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

Brazil is already a large market for cloud providers, with its figures drastically increasing each year.

According to a recent research by Citrix (referenced in this article: https://computerworld.com.br/2018/08/30/brasil-ampliara-investimento-em-cloud-em-linha-com-cenarios-futuros/ and https://exame.abril.com.br/negocios/dino/us-43-bilhoes-de-um-lado-us-93-bilhoes-de-outro-cloud-e-seguranca-destacam-empresas-brasileiras/), 57 per cent of Brazilian companies already adopt cloud computer solutions for their businesses. Moreover, 74 per cent of Brazilian companies intend to invest in cloud technologies in the near future and to integrate services and applications to a cloud in the next three years.

The International Data Corporation estimated that, in 2017, investment in the cloud computing sector reached approximately US$20 billion (https://exame.abril.com.br/negocios/dino/us-43-bilhoes-de-um-lado-us-93-bilhoes-de-outro-cloud-e-seguranca-destacam-empresas-brasileiras/).

According to a 2019 study published by the Brazilian Association of Software Companies (ABES) (http://central.abessoftware.com.br/Content/UploadedFiles/Arquivos/Dados%202011/ABES-EstudoMercadoBrasileirodeSoftware2019.pdf), the public cloud market in Brazil was expected to reach US$2.3 billion and grow 35.5 per cent per year until it reaches US$5.8 billion in 2022.

However, a portion of Brazilian companies still do not completely trust the security of the cloud computing model and fear being dependent on a service provider (lock-in). They view the quality of telecommunications infrastructure as a limitation for adopting cloud-based solutions (www.la.logicalis.com/globalassets/latin-america/advisors/pt/_it_snapshot_2018_web.pdf).

Impact studies

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

Publicly available research on the impact of cloud computing in Brazil is primarily developed by private entities, with a few exceptions published by the government. A recent study by Logicalis (a private consulting entity) predicts an optimistic future for the IT market (www.la.logicalis.com/globalassets/latin-america/advisors/pt/_it_snapshot_2018_web.pdf).

According to this research, half of the Brazilian companies that were interviewed have IT solution budgets 14 per cent higher in 2018 than 2017, while 34 per cent of companies expect to keep the same level of investment as 2017.

The Brazilian Association of Software Companies – ABES also publishes studies with overviews and trends for the Brazilian software market that contains data about cloud-based solutions. The last edition of such study was published in 2019 with data from 2018 (http://central.abessoftware.com.br/Content/UploadedFiles/Arquivos/Dados%202011/ABES-EstudoMercadoBrasileirodeSoftware2019.pdf).

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 government is taking steps to encourage the development and dissemination of new technologies, including cloud computing. One initiative is a federal programme called the Strategic Program for Software and IT Services.

The government issued a statement in 2012 stating that it planned to invest 486 million reais in this sector alone (40 million real only for start-ups and 446 million reais for companies that develop software for certain industries) and, in 2014, six major technology companies entered into memoranda of understanding with the Ministry of Science, Technology and Innovation to instal research and development centres in Brazil.

Other government programmes, such as 'Brasil Mais TI', are also targeted at developing its students' IT-related skills, including those related to programming, the internet and cloud.

Additionally, in 2016, the federal government published a guide to assist public bodies in contracting cloud computing services (www.governodigital.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf). This guide included recommendations for data to be kept on Brazilian territory and for the adoption of a hybrid cloud solution for cases that do not compromise national security.

The fact that a public bid was opened in 2018 and, in January 2019, resulted in the award of a 29.9 million reais agreement to a private company to provide cloud services to several government agencies also reflects the fact that public authorities may shift their focus to cloud-related services in the coming years.

Incentives

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

Currently, there are no specific fiscal or customs incentives for cloud computing in Brazil. Nor is there a definition on which tax is applicable – if ICMS (a VAT-like tax) should apply, which is collected by Brazilian states, or if ISS (service tax) should apply, which is collected by Brazilian municipalities.

If the service tax ends up prevailing, then there is an indirect incentive for cloud service providers to be located in the Brazilian territory (ie, a local entity as the cloud provider) since the amount of taxes applicable to providers located abroad are significant for importation of services.

After there is a definition on which tax is applicable to cloud computing solutions, it is very likely that Brazilian states (in case of VAT-like tax) or municipalities (in the case of service tax) will create tax incentives to bring service providers to their locations.

See questions 24 and 25 for more tax-related information.

The Ministry of Economics issued this April 2019 Normative Instruction No. 1/2019, which sets forth rules for the contracting of information and communication technology solutions by certain public entities. This Normative Instruction provides that, if public entities need to create, improve or renew their datacentre infrastructure, they should opt for cloud computing, unless such option is not viable according to pre-contractual studies. This means that even the government is favouring cloud computing services in lieu of other solutions.

LEGISLATION AND REGULATION

Recognition of concept

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

There is no express reference to cloud computing in Brazilian federal laws. However, the Brazilian Central Bank issued Resolution No. 4,658 on 26 April 2018, which sets forth requisites for processing and storing data and for cloud computing solutions for information collected by financial institutions (see question 13).

Although there are no laws referencing cloud computing, the Information Security Cabinet of the President's Office and the Ministry of Planning, Budget and Management (which is now part of the Ministry of Economics) issued in 2018 and 2016, respectively, a complementary norm and a general guideline with norms and best practices to be followed by federal entities in contracting cloud computing services. Cloud computing is defined in such documents as a computational model that allows access on-demand, independently of where it is located, to computational resources (network, servers, hosting, applications and services) provided and made available with minimal management efforts or interactions with the service provider.

The Ministry of Economics also issued in April 2019 Normative Instruction No. 1/2019, which provides that certain public entities must favour cloud-based services for their datacentre infrastructure, and explicitly references the President Office's complementary norm indicated above.

There are federal laws that apply specifically to internet operations and to data protection, which impact cloud computing and their providers.

The Brazilian Civil Rights Framework for the Internet (Federal Law No. 12,965/2014 (the MCI)), which was further regulated by Federal Decree No. 8,771/2016, provides for principles, rights and obligations regarding the use of the internet in Brazil, and sets forth obligations for internet connection and application providers, which are relevant for cloud computing solutions in general.

Recently, the Brazilian General Data Protection Act (Federal Law No. 13,709/2018 (the BR GDPA)) was sanctioned and will come into force in August 2020. The BR GDPA will apply irrespective of industry or business when personal data is collected or processed. Among other norms, it provides for user consent for the collection, processing and transfer of data (with specific provisions pertaining cross-border transfer), data security and data breaches, sensitive personal data and situations for ceasing the processing of data.

Governing legislation

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

Brazilian legislation does not directly and specifically prohibit or restrict cloud computing services, either in or outside Brazil.

In 2018, the Brazilian Central Bank issued Resolution No. 4,658, which provides for precautions to be taken by financial institutions in

contracting cloud services and for the responsibility of such institutions for the reliability, integrity, availability, security and confidentiality of the contracted cloud services. The financial institution must notify the Central Bank prior to contracting the services and certain requirements must be met for the cloud service to be rendered abroad.

See questions 8 and 10 for information on norms applicable to cloud computing and internet-based services.

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

The MCI provides for rights and obligations for different stakeholders on the internet and sets forth parameters for the protection of user data. The MCI is applicable to internet connection and application providers in general. It provides for a vague and broad definition of internet application providers ('a set of features that might be accessed through a computer connected to the internet'), which potentially makes cloud computing services and their providers subject to such legislation.

General requirements are related to the following obligations and provisions:

- access logs data retention by internet application providers;
- users' rights in connection with personal data;
- agreement provisions that might be considered void under Brazilian law;
- obligation to provide information on data processing activities;
- data request by Brazilian authorities; and
- liability for content created by third parties.

The BR GDPA will be applicable irrespective of industry or business when it comes to the processing of personal data. Among other norms, it provides for user consent for the collection, processing and transfer of data (with specific provisions pertaining cross-border transfer), data security and data breaches, sensitive personal data and situations for ceasing the processing of data.

It is also worth mentioning Federal Decree No. 9,637/2018, which disciplined the National Information Security Policy and created the Information Security Management Committee, a government body that advises the Institutional Security Cabinet of the President's Office in information security-related matters.

Breach of laws

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

According to the MCI, if an internet application provider (in which category cloud computing providers are included) fails to comply with a take-down order issued by a court (or with an extrajudicial letter sent by an affected party in case of pornography or sexual content), it may be held liable for content created by third parties. Thus, the MCI established a safe harbour for such situations, by which an application provider is not held liable before it is notified either by a party or by a judge.

If the application provider fails to comply with a court order or extrajudicial letter, it would likely be sentenced to pay an indemnification for material or moral rights to the aggrieved party, depending on the facts of the case (there are several types of content that may be deemed unlawful under Brazilian law, the most common types being defamation, racism, child pornography, bullying, rights of publicity and other personality rights).

The MCI also provides for penalties of warning; administrative fines of up to 10 per cent of the income of the economic group in Brazil, net of taxes, to be calculated according to the economic condition of the offender and the principle of proportionality between the severity of the offence and the intensity of the penalty; and suspension or prohibition of the activities pertaining to the collection, storage or processing of logs, personal data or communications.

Apart from administrative fines that may be imposed according to the MCI, courts can impose fines for non-compliance with preliminary injunctions or final decisions ordering the removal of content or the producing of data. There is no limit on such penalties, which are set by judges on a case-by-case basis. Courts may also award damages if the company fails to obey the court order to remove the content.

If the company does not take down a specific content after a court order, this could be considered a crime of 'disobedience' (article 330 of the Brazilian Criminal Code), the penalty for which is 15 days' to six months' imprisonment (for officers or administrators) and a fine. The risk of criminal liability is higher in matters involving criminal organisations or child pornography.

Regarding infringements to the provisions of the BR GDPA, in addition to liability for moral and material damages, data-processing agents are subject to the following administrative sanctions: warning with a deadline implementing corrective measures; fine of up to two per cent of the revenues earned by the legal entity, group or conglomerate in Brazil in the preceding year, net of taxes, capped at 50 million reais per offence; daily fine, subject to the cap referred to above; disclosure of the offence after the occurrence thereof having being investigated and confirmed; blocking of the personal data to which the offence refers, until the processing activity is regularised; and deletion of the personal data related to the infringement.

Consumer protection measures

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

Legal consumer relations in Brazil are regulated by Law No. 8,078/1990 (the Consumer Protection Code or CDC), which governs all consumer relationships, including cloud computing products or services where there is a supplier on one side and a consumer on the other side. 'Consumer' for this purpose is defined as any individual or legal entity that acquires or uses products or services as an end user.

The CDC protects consumers and, in general, its language allows consumers to file claims against companies involved in the supply chain. If an entity is not directly responsible for damage suffered by the consumer, such company may seek the amount paid by it to the consumer from the other liable company.

The CDC sets forth a 30-day or 90-day deadline for the consumer to file a suit pertaining to a defective product or service and a five-year period for damages caused to the consumer's physical or mental health.

The supplier (where the consumer is an individual) cannot disclaim or limit its liability for product or service defects, and all contractual clauses with this language will be null and void. The agreement also cannot include clauses impairing, disclaiming or mitigating obligations to indemnify. There is no legal restriction on the warranty term apart from the 30-day or 90-day terms counted from the delivery of the product or from the rendering of the service, by any contractual warranty must be clear, precise and additional to the legal warranty.

The CDC also provides for a right to regret, by which consumers have the prerogative to return a product or a service contracted outside the point of sale within seven days of delivery. Currently, this rule applies to purchases made through the internet, where the consumer has no physical contact with the product or service.

Choice of foreign law and arbitration or foreign venue clauses in consumer contracts are usually held null and void by Brazilian courts, especially small claims courts, because they tend to complicate the consumer's pursuit of his or her rights. However, in a 2018 decision,

the Superior Court of Justice considered that the nullity of a choice of venue clause (where the elected venue was a different city of the same Brazilian state) was contingent on the proof of harm to the consumer's ability to claim his or her rights.

Sector-specific legislation

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

The Brazilian Central Bank issued Resolution No. 4,658 on 26 April 2018, which sets forth requisites for processing and storing data and for cloud computing activities related to information collected by financial institutions.

Resolution No. 4,658/18 sets forth that the outsourcing of relevant data processing, storage and cloud computing services must be communicated in advance by the financial institution to the Central Bank. Such communication must comprise the name of the service provider, the service being outsourced and the indication of the countries where the services may be rendered and the data may be stored and processed.

The financial institution contracting cloud services must implement procedures to verify the service provider's ability (companies that offer cloud computing, data storage and processing services to financial institutions) to ensure:

- compliance with prevailing laws and regulations;
- the institution's access to the data and information to be processed or stored by the service provider;
- the confidentiality, integrity, availability and recovery of data and information being processed or stored by the service provider;
- the service provider's adherence to certifications required by the institution for outsourcing of the corresponding services;
- the institution's access to reports prepared by an independent expert audit company hired by the service provider concerning the controls and procedures being adopted for outsourced services;
- the availability of management information and resources competent for monitoring the outsourced services;
- the identification and segregation of data belonging to the institution's clients, via physical or logical controls; and
- the quality of access controls targeted at protecting the data and information referring to the institution's clients.

For contracts with entities of the public administration regarding services related to datacentre infrastructure, there are rules favouring the contracting of cloud-based solutions, as mentioned in questions 7 and 8.

Insolvency laws

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

There are no insolvency laws in the Brazilian legal system that apply specifically to cloud computing. The general provisions governing liquidation and recovery in insolvency proceedings are provided for in Federal Law No. 11,101/2005 (the Insolvency Act).

The Insolvency Act sets forth which credits or creditors have precedence over others in insolvency or credit recovery, and a Brazilian customer seeking to enforce rights against an insolvent cloud computing provider would have to follow the regular procedures, being in general a regular creditor (unless there is a specific guarantee with respect to the services provided). Micro or small companies, for instance, have certain benefits (representation in general meetings, for example) and their credits come before general unprivileged credits.

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.

The BR GDPA is the main norm to be applicable (after August 2020) to any personal data processing activity in Brazil. It will create a robust legal landscape for personal data processing and will strengthen data subjects' rights in relation to their personal data. It applies irrespective of industry or business when it comes to the processing of personal data. Among other norms, it provides for user consent for the collection, processing and transfer of data (with specific provisions pertaining cross-border transfer), data security and data breaches, sensitive personal data and situations for ceasing the processing of data.

It also provides to the implementation of controlled processes to ensure data subjects' rights, such as the rights to access, correction, anonymisation, blocking, deletion and portability of personal data, as well as provide for the possibility of creation of several documents by companies, including privacy policies, consent forms, internal manuals, agreements with data operators and companies with whom it shares collected personal data, documentation supporting cross-border transfers of personal data and impact assessment reports.

Additionally, there are provisions of the MCI and the Federal Decree No. 8,771/2016 that are applicable to data processing in general, including cloud computing providers. Such provisions include obligations to keep access logs for a minimum period of time; to obtain consent for the processing of personal data (and such processing must be adequate and clear); to use the data only for the purposes that justify its collection; and to delete the collected personal data as soon as its processing is finished.

General provisions provided by sparse laws may also be applicable depending on the issue involved (eg. for consumer relationships, the Consumer Protection Code will apply).

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)?

There are a few main forms of cloud computing contracts usually adopted in Brazil: infrastructure-as-a-Service (IaaS, where the contracting party seeks to rent IT infrastructure usually for the processing, storing or transferring of data); platform-as-a-Service (PaaS, mainly for developing, delivering and managing software applications); and Software-as-a-Service (SaaS, for a wide range of activities, including communications, collaboration, productivity, customer management, taxing and account activities etc).

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?

In B2B contracts, parties are generally free to choose the applicable law and to elect a venue for dispute resolution. When the parties to the contract are all Brazilian entities, the governing law and the venue chosen for dispute resolutions are usually Brazilian.

When the cloud computing provider is not a Brazilian entity (eg, when the provider does not have operations in Brazil or when its local

entity is only for marketing, implementation or maintenance), the parties may negotiate different applicable law and dispute resolution clauses, including foreign law and foreign courts or arbitration tribunals.

However, the MCI provides that, in adhesion agreements, where the terms of the agreement are standard and the contracting party is not able to negotiate its clauses, any foreign forum selection clause for disputes arising out of services rendered in Brazil will be null and void.

Under the CDC, a company could be considered a consumer if it acquires the product or service as an end user and it is vulnerable when compared with the supplier of products or services, so the CDC may also apply in B2B contracts. In this case, any provision that limits or impairs the consumer's pursuit of rights (such as the election of foreign law or foreign courts or arbitration) is likely to be considered null and void by Brazilian courts.

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?

In general, cloud computing services are paid for on a monthly basis, and prices can be either a fixed amount or an amount according to the volume of use (eg, the amount of data stored or processed). The agreements may include regular monetary adjustments according to national inflation indexes.

Service level agreements are also common, and they usually provide for minimum efficiency levels and discounts or penalties in case such levels are not met.

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?

Cloud computing contracts usually cover security measures applicable to data, especially personal data collected by a party. These security measures may comprise data isolation, minimum standards and parameters, encryption and backups.

Some companies provide in their contracts that the data will be kept in servers in Brazilian territory (which may be a requirement for public contracting entities).

After the MCI, companies have been including consent clauses in their agreements to support their collection and processing of personal data. This will be strengthened and more detailed in contracts until August 2020, when the BR GDPA enters into force and the companies' practices will need to comply with its provisions, so changes to the standard cloud computing agreements are expected by then.

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?

Parties are generally free to negotiate clauses covering liability, warranties and provision of service. Thus, liability or indemnification caps are common, as well as warranties for the rendered services and service level agreements with a minimum level of service to be met by the provider.

If the clauses are abusive, especially if the contracting party is vulnerable and not able to negotiate the contract terms (eg, in the case of an adhesion contract), they could be considered null and void in litigation. This could be the case for small liability caps that do not cover a substantial amount of the damage caused by a provider to the contracting party.

Finally, the CDC (which may apply to agreements entered into by legal entities) provides that, although any clause that limits the responsibility of the supplier for damage caused to individual consumers will be null, this is not the case for consumer relationships where the consumer is a legal entity and there is justification for the limitation of liability.

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 agreements usually provide that there will be no transfer of ownership and that all intellectual property will be held by the party who owns it in the first place.

This means that the cloud computing provider will keep all intellectual property related to the provision of services and to the technology related to the services, and the customer will keep all intellectual property on the content that it provides for the services to be rendered (for example, the content uploaded to a cloud storage).

It is also common to include in contracts clauses by which the customer declares that it is responsible for the content that it provides for the rendering of services, and that it shall not infringe any third-party rights (eg, that the customer will not keep infringing material in cloud storage).

In the case of third-party intellectual property infringement, the parties usually agree that the infringing party will indemnify the other in case it is held liable.

Also common is the inclusion of clauses by which the customer declares to be responsible for any content that it uploads to or create in the cloud. This is supported by a safe harbour provision of the MCI according to which an application provider (ie, the cloud provider) will only be liable in the civil sphere for damages caused by content created by third parties (ie, customers) if it fails to remove such content after a specific court order, to the extent technically possible, or after received notice, in case of sexual-related content. Copyright infringement is not explicitly covered by the MCI provision until a specific legal provision is passed.

Typical terms covering termination

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

Termination clauses depend on the nature of services being rendered. While certain agreements allow for any party to terminate at any time, others may provide for predetermined agreement terms or extension cycles (eg, one-year terms extendable for successive one-year terms) with certain periods for termination notices (eg, at least 30 days before the end of the current term). In this situation, there could be penalties where the agreement is terminated early or not in accordance with the procedure set forth in the termination clause.

Typically, termination clauses cover the return or destruction of the data provided by the customer under the agreement in a safe manner to ensure that no data will be lost or unduly breached by third parties, and confidentiality terms will apply to both parties for an indefinite or limited amount of time.

The MCI obliges all internet application providers (and such definition comprises cloud computing providers) to keep internet application access logs for a minimum of six months, and some companies include this data retention in their agreements to inform their customers about this legal obligation.

The BR GDPA provides that personal data should be deleted after its processing purpose has been reached, with a few exceptions, which include transfer to third parties and exclusive use of anonymised data. This matter can be included in a termination clause in case the cloud computing provider wishes to use data after the termination of the agreement, provided that all limitations under the BR GDPA are met.

Employment law considerations

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

There are no specific labour laws applicable to cloud computing.

If, in a specific contractual situation, cloud computing is considered as not a mere provision of services but as an outsourcing of the workforce for the contracting party, then certain labour laws could apply. In this case, if the cloud computing provider fails to pay its employees their wages and benefits, the contracting party could be held responsible and be obliged to fulfil such labour law obligations.

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 providers are subject to the corporate income tax and the social contribution on net profits at the joint rate of 34 per cent, as well as the contribution to the profit participation programme (PIS) and the social security financing (COFINS), at 9.25 per cent (over total revenue) under the non-cumulative regime or 3.65 per cent under the cumulative regime.

Based on the nature of cloud services, revenues should be subject to the non-cumulative PIS and COFINS regime with the application of the 9.25 per cent rate and the possibility of using credits.

If the cloud services are imported from outside, remittances are subject to the withholding tax at a 15 per cent rate (or 25 per cent, if the beneficiary is located in a tax haven jurisdiction). Tax authorities have recently manifested themselves, when analysing the taxation of remittances related to the resale of SaaS, that such remittances should be classified as technical services subject to the federal contribution (CIDE) at a 10 per cent rate, and to the PIS/COFINS at the combined 9.25 per cent rate.

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.

The most relevant analysis from a Brazilian tax perspective is whether cloud computing services are subject to ICMS or to ISS (service tax). Both ISS and ICMS are consumption taxes.

ICMS is assessed over the sale of goods and the provision of communication and transport services. Recent modifications in the legislation regulated the procedures for charging ICMS for transactions related to digital goods.

ISS, in turn, is a service tax assessed over any service (except those subject to ICMS) as long as the service is provided for in a list of services attached to Complementary Law 116/2003.

Item 1.03 of Complementary Law 116/2003 includes processing, storage of hosting of data, texts, images, videos, web pages, apps, information systems, among other forms, and congeners in the list of services taxed by ISS, and these activities are at the heart of cloud computing.

It is currently not clear which tax should apply to such digital activities, fuelled by a dispute between Brazilian states and municipalities, because ICMS is collected by the former and ISS by the latter.

Specifically regarding SaaS activities, the Tax Authorities of the municipality of São Paulo published Normative Ruling No. 1/17 stating that SaaS activities are subject to ISS based on item 1.05 (software licensing) of the list of services of Complementary Law 116/2003.

In this same Normative Ruling, authorities also recognised the hybrid nature of SaaS activities and, consequently, the possibility of it encompassing additional services classified on items 1.03 (indicated above) and 1.07 (technical support in IT, including the installation, configuration and maintenance of computer programs and databases).

The consumption taxes mentioned above are applicable if the service is provided from within or imported from outside.

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.

In September 2018, Engineering do Brasil, SAP and Google Cloud announced a commercial partnership to promote innovative solutions using artificial intelligence, machine learning and cloud computing. These three companies are working on an artificial intelligence that assists other companies in managing their tax obligations. For this project, the objective is to integrate the technologies provided by Google Cloud and SAP with Engineering do Brasil's tax expertise.

Another notable commercial partnership was entered into in 2017 by Microsoft and Infraero, a state-owned organisation responsible for managing Brazilian commercial airports. Both companies developed a cloud-based corporate social network to unite employees of the Brazilian company. The network aims to improve the communication and collaboration between Infraero teams and directors.

The Brazilian Central Bank is also interested in regulating and incentivising cloud computing technologies, which is evident from this year's issuance of Resolution No. 4,658 and from the creation of a Technological Financial Innovation Lab, coordinated by the Central Bank, which has AWS, IBM, Microsoft and Oracle (relevant companies in the provision of cloud computing services) as supporters.

In January 2019, Primesys/Embratel was awarded, after a bid in which numerous Brazilian and foreign companies participated, an agreement with the public administration for the rendering of cloud computing services. The value of the contract is 29.9 million reais.

In April 2019, the Ministry of Economics issued a Normative Instruction setting forth rules for the contraction of information technology solutions by public entities. Among several provisions, there is one by which cloud computing must be favoured for the creation, improvement or renewal of datacentre infrastructure, unless it is not a viable option according to technical studies.

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?

Currently, one of the main challenges for cloud computing providers (and for companies in general) in Brazil is conforming to its business practices according to obligations and customer rights set forth in the BR GDPA, which, in many cases, involve costly and comprehensive adaptations and investments in security measures. This will be either facilitated or complicated after the effective creation of the Brazilian Data Protection Authority, which shall have the power to enact specific norms and guidelines to supplement the general rules of the BR GDPA and to create additional obligations on companies of specific sectors.

Also challenging is the decision as to which consumption tax should apply to digital or cloud services, whether ICMS or ISS (see question 25), since Brazilian states and municipalities still do not agree and tend to tax companies according to their local rules.

PINHEIRONETO
ADVOGADOS

José Mauro Decoussau Machado
jmachado@pn.com.br

Ana Carpinetti
acarpinetti@pn.com.br

Gustavo Gonçalves Ferrer
gferrer@pn.com.br

Rua Hungria 1100
São Paulo 01455-906
Brazil
Tel: +55 11 3247 8400
Fax: +55 11 3247 8600
www.pinheironeto.com.br

France

Olivier de Courcel and Stéphanie Foulgoc Féral-Schuhl/Sainte-Marie
Alain Recoules Arsene Taxand

MARKET OVERVIEW

Kinds of transaction

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

The official statistics define 'cloud computing' as the IT services used on the internet to access a software, processing power or a storage capacity and that include all the following characteristics:

- to be delivered from IT servers operated by service providers;
- to be easily increased or decreased;
- once installed, to enable use without the need for human contact with the provider; and
- to be payable either by the user or depending on the capacity used or to be prepaid.

These services may include connections via a virtual private network (VPN) (https://www.insee.fr/fr/statistiques/3856105?sommaire).

The different varieties of cloud computing services covered by this definition are offered in France. In 2018, the services the most frequently used were infrastructure-as-a-service (IaaS, according to the NIST typology), mainly in the form of file storage (27,002 companies out of the reportedly 35,280 using cloud computing services). Software-as-a-service (SaaS) was also very frequently used by businesses (mainly for messaging services; otherwise, for office automation software, customer relationship management and accounting software), just as much as database hosting (in the platform-as-a-service (PaaS) category) (Insee, TIC 2018 enquiry, TAB08: Use of cloud computing services by internet).

Furthermore, according to the same statistical enquiry, in 2018 the businesses that purchase cloud computing services on shared IT servers (public cloud) are almost as numerous as those requesting servers exclusively reserved for their needs (private cloud).

Active global providers

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

Amazon Web Services enjoys a dominant position in France like elsewhere, and the other principal global providers, Microsoft Azure and Google Cloud Platform, are also very active (www.lesechos.fr/tech-medias/hightech/google-cloud-sera-aussi-gros-quamazon-web-services-dans-deux-ans-1030266). Numerous other international players commercialise their services directly or indirectly in the country (eg, IBM, Rackspace, Oracle, NTT, Salesforce, Alibaba, Tencent) (https://www.zdnet.fr/actualites/top-2019-des-fournisseurs-de-cloud-aws-azure-gcp-ibm-sur-l-hybride-et-salesforce-domine-le-saas-39880577.htm).

Active local providers

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

While the principal global providers are dominant players on the market for both the software-, platform- and infrastructure-as-a-service activities, in France this market includes pure players such as OVH and Outscale (IaaS and PaaS) as well as providers integrating both public and private cloud services offerings such as Atos, Orange, Capgemini and Sopra Steria (www.usinenouvelle.com/article/atos-tire-30-de-son-chiffre-d-affaires-2018-du-digital-pas-assez-pour-dynamiser-sa-croissance/). As there are numerous providers active in France, some of them can be found among the members of the EuroCloud association (www.eurocloud.fr/adherents/) (SaaS, PaaS) or of the Cloud Infrastructure Services Providers in Europe association (CISPE: https://cispe.cloud/publicregister) (IaaS).

Market size

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

According to the official statistics (see question 1), 19 per cent of French companies with at least 10 employees were using cloud computing services in 2018.

The research firm Markess published a barometer estimating the size of the French cloud computing market to be nearly €12 billion in 2019, representing a growth of 20 per cent over the previous year (www.usinenouvelle.com/article/le-cloud-en-france-un-pactole-de-12-milliards-d-euros-en-2019.N862810).

Impact studies

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

Numerous analyses and official studies are regularly undertaken on the digital sector in France including, more specifically, on cloud computing services. The INSEE statistics (www.insee.fr) and the analyses of the Ministry of Economy and Finance (www.entreprises.gouv.fr/observatoire-du-numerique/usages) are the most prominent ones.

The administration is particularly focused on the modus operandi for the different forms of cloud computing and publishes its works for the needs of the public bodies (for example, www.entreprises.gouv.fr/numerique/guide-du-cloud-computing-et-des-datacenters).

Ad hoc analyses are undertaken by professional organisations such as EuroCloud (www.eurocloud.fr), which includes 200 service providers on the cloud market, or Syntec Numérique, which represents digital service companies, software publishers and technology consultancy companies (www.syntec-numerique.fr). On the side of users, associations such as Cigref (www.cigref.fr) or software user clubs such as SAP's (www.usf.fr) also publish such analyses.

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?

Successive governments express concern about the security of data originating from their administrations and other public bodies. In 2012, the government encouraged the creation of two data hosting providers, Cloudwatt and Numergy, to enable data storage on national territory, out of reach of foreign legislations and extraterritorial access by foreign governments ('sovereign cloud'). Yet, this initiative was short-lived as major public customers prefer major classic players (for example, the national railways, the city council of Paris, the Ministry of Defence – see www.lesechos.fr/idees-debats/cercle/le-secteur-public-a-besoin-dun-cloud-souverain; www.zdnet.fr/actualites/, microsoft-et-ministere-de-la-defense-le-debat-sur-le-contrat-open-bar-fait-son-retour/).

Beyond such concerns for data security, cloud computing is one of the hot topics in every new government economic development plan (eg, 'Nouvelle France Industrielle', 2013; 'Grand plan d'Investissement', 2017…).

Incentives

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

Although not limited to such operations, various financial funding and tax benefits may help support investments in cloud computing activities.

Specifically, financial funding for innovation and loans may be granted in the context of the Investment Plan for Europe (the Juncker Plan) and of the 'FrenchTech' programme in support of start-ups. These programmes are managed by the public agencies usually in charge of financing the economy, the Deposits and Consignments Fund (www.caissedesdepots.fr/developper-le-numerique-sur-le-territoire) and BPIFrance (www.bpifrance.fr/A-la-une/Actualites/Systancia-securise-les-applications-dans-le-cloud-35047).

Preferential tax benefits such as the tax credit on research and development costs, the tax exemption for innovative new companies or the tax credit for innovation expenses may also be called upon under their own terms.

LEGISLATION AND REGULATION

Recognition of concept

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

The concept of cloud computing has been acknowledged by the official texts since 2010, when the terminology commission in charge of establishing the official definition of new terms in the French language defined 'cloud computing' (that is, a 'means of processing client data, the exploitation of which is made via internet, in the form of services provided by a service provider') and provided an official translation in the French language.

For the purpose of implementing the EU directive on Network and Information System Security of 9 July 2016, the French legislator enacted in February 2018 a statutory definition of the 'cloud computing service' (that is, 'a digital service that enables access to a set of flexible and variable IT resources that may be shared'). This service is classified among the 'digital services', along with online platforms and search engines, for which the providers are obliged to comply with certain security obligations (see question 9).

Governing legislation

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

The Law No. 2018-133 dated 26 February 2018 transposed Directive No. 2016/1148 of the European Parliament and the Council dated 6 July 2016, which aims to meet a uniform high level of security for the networks and information systems set up in the EU (NIS).

This law obliges digital services providers (including cloud computing providers) to identify the risks that affect their networks and information systems' security and to take the technical and organisational measures necessary for managing these risks, to guarantee the continuity of their services.

These providers must notify the National Cybersecurity Agency (ANSSI) of any incident that has a significant impact on the provision of their services. Upon the Prime Minister's initiative, they may be subject to compliance and security controls, which will be made by the same agency. When they offer their services in the EU but are located in a third-party state, such providers must designate a representative in a member state.

Further to the adoption of the General Data Protection Regulation (GDPR) (see question 15), the EU enacted on 14 November 2018 Regulation No. 2018/1807, which establishes a framework for the free flow of non-personal data within the EU. Specifically, this text prohibits member states from requiring the localisation on their territory of the processing of data that is neither personal data nor 'inextricably linked' to personal data. Exceptions are allowed only if based on public safety grounds and balanced accordingly and must be reported to the EU Commission by 30 May 2021. These provisions will concern, in particular, the use of cloud computing services by state administrations and other public bodies, whose data are currently considered as 'public archives' and must not be exported out of the territory (Heritage Code, article L111-7).

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

Posts and Electronic Communications Code (CPCE) (telecom operators)

Under the existing EU 'telecom package,' services relating to digital 'content' provided online (eg, online platforms, search engines, site hosting, portal management, edition of online content, etc) are distinguished from telecommunication services, which concern the 'container'. Telecommunication operators are governed by their own provisions which, historically, have been more burdensome than those applicable to cloud and other digital services providers, for instance, as regards internet neutrality (governed by EU Regulation No. 2015/2120 dated 25 November 2015), personal data protection, confidentiality of correspondence, neutrality in respect of messages content or access to emergency numbers. Yet, in practice, the boundaries between services are not as obvious. For instance, the main digital services providers set up cache servers in the operators' networks in order to bring their content closer to end customers. Accordingly, about 50 per cent of the incoming traffic to internet access providers originate from the four main content providers – Google, Netflix, Akamai, Facebook (Regulatory Authority for Telecommunications (ARCEP), 2019 Report). It was not until recently that the European Court of Justice itself had to determine whether Skype should be considered as a telecommunication service

and fall within the telecommunication regulatory regime (ECJ, No. C142-18, *Skype Communications Sarl v IBPT*, 5 June 2019).

The forthcoming EU Electronic Communications Code (due to be transposed by the member states by 21 December 2020) attempts to restore fairer competition conditions. It will cover the existing telecommunications services but also 'interpersonal communications services', regardless of whether users connect through publicly assigned numbering resources or otherwise. Voice over IP and messaging SaaS services such as Skype, WhatsApp, Wechat or Facebook Messenger should, therefore, fall within the scope of the regulated services.

On another note, the CPCE defines and regulates a service category which combines both telecom and cloud computing aspects, the 'electronic safe'. The purpose of this service is the receipt, storage, removal and transmission of data and electronic documents in conditions that must retain their integrity and exactitude of origin (article L.103). The providers of these services must set up the security measures necessary to meet these conditions and to ensure the traceability of the operations made on the data and documents. They must set up a technical file to provide proof of their adherence to the legal requirements.

Defence Code (Fundamental Operators)

Since the law of military programming No. 2013-1168 dated 18 September 2013, the Defence Code submits a specific category of players, the infrastructures and systems of which are strategic for the country, designated as Fundamental Operators (OIV), to specific rules concerning the security of their information systems (article L1332-6-1 et seq). Each OIV is obliged to provide a map of its information system, ensure that it is homologated and establish a security policy for its system. The OIVs must inform the Prime Minister of the incidents affecting the functioning or security of their information systems. They must enable the ANSSI to carry out audits and must set up any security measures requested by the latter. Such obligations require the service agreements to be adapted, including those that they may enter into with digital service providers for cloud computing.

General tax code (clients)

All companies are obliged to retain the documents on which the French tax authorities have a right of communication, enquiry and control. The documents in question must be kept for at least six years (Tax Procedure Code, article L102 B). In this context, the use of a cloud computing service to store invoices must meet the various conditions concerning the terms of conservation of the documents and the countries of location of the storage servers (Tax Procedure Code, article L102 C). The invoices issued or received by a company must remain accessible from its principal establishment or registered office in France, regardless of the country of storage. The French tax authorities must be informed of the location of storage of the invoices.

Furthermore, when an accounting department works with automated systems (including SaaS), the tax authorities' right of control applies to all the information, data and software processing that are used to establish the results and statements for the tax authorities, as well as the documentation relating to the analysis, programming and the performance of IT processing (Tax Procedure Code, articles L13, IV and L47 A,II).

For such a purpose, the tax authority may set up its own IT processing on the company's equipment. Furthermore, since 2014, all companies must communicate their online accounting to the tax authorities according to the required standards (Fichier des Ecritures Comptables). Finally, the tax authority may, after court authorisation, launch a search and seizure procedure, including the seizure of data hosted on IT servers. The location abroad of the servers concerned does not constitute an excuse (Paris Court of Appeal, order dated 31 August 2012).

Others

Other examples may be found in a variety of texts, including the second version of the European Payment Services Directive (PSD2), which entered into force in January 2018 and makes strong authentication mandatory for payments over €30.

Furthermore, cloud computing transactions are indirectly governed by sector-specific legislation or regulations, as discussed in question 13, as well as by data protection and privacy legislation applicable to any kind of personal data processing, as discussed in question 15.

More generally, all regulations governing business-to-business (B2B) relations apply to transactions between cloud computing service providers and businesses. For instance, the French Law No. 2016-1691 on transparency, fight against corruption and modernisation of the economy of 9 December 2016 (Sapin II Law) requires large businesses to take measures to prevent and detect acts of corruption and subornation. Cloud computing records will be key to demonstrating compliance.

Breach of laws

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

The Law No. 2018-133 dated 26 February 2018 (see question 9) sanctions the directors of digital service providers to a fine of €100,000 when they prevent audit and security operations from being carried out in accordance with the law, and a fine of €75,000 when they do not comply with security measures that they have been formally required to take as a result of such an audit. If they fail to declare an incident or disclose information to the public as legally required, these directors may be subject to a fine of €50,000.

The Posts and Electronic Communications Code sanctions operators and their agents to a one-year prison sentence and a fine of €75,000 for failure to delete or ensure the anonymity of any data relating to communications or for not retaining technical communication data in accordance with the legal requirements (article L39-3) (see question 10). Furthermore, those who offer a connection to the public enabling an online communication via an internet access, including for free, are required to comply with the provisions applicable to telecoms operators, including to register themselves with the competent regulatory authority (ARCEP). Accordingly, they are subject to the same sanctions as telecoms operators (article L34-1).

The Defence Code sanctions directors of the OIVs to a fine of €150,000 if they fail to set up a protection plan, to accomplish works they have scheduled or to carry out the works requested following an audit, or otherwise fail to comply with their legal obligations (article L1332-7). These sanctions may be multiplied fivefold for the operators as legal persons.

Consumer protection measures

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

With regard to consumers, the cloud computing service providers are obliged to respect the provisions of the Consumer Code. This code regulates the entire relationship with a client, from the obligation to provide pre-contractual information (article L111-1 et seq), the process for entering into an online contract (article L121-16), the prohibition or regulation of commercial practices and abusive clauses, the provision of guarantees, through to the terms for terminating such contracts.

The pre-contractual information must be provided in a legible and understandable manner and a written confirmation of the contract must be provided as well (article L221-5). Insofar as the request for cloud computing services usually implies immediate use, the usual right of

withdrawal that lasts for 14 days will most often not apply (article L121-21-8 1°). Finally, the consumers benefit from a right of portability of their personal data within the conditions of the GDPR (see question 15).

Sector-specific legislation

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

A number of sector-specific legislation or regulations that do not specifically target cloud computing transactions actually apply indirectly thereto. In regulated sectors (eg, healthcare, banking, etc), regulations or recommendations in this respect are usually issued by the authority in charge of the sector. The following provides only a few examples.

General Security Referential (public sector)

Since Decree No. 2010-112 dated 2 February 2010, the state administrations, local authorities and other administrative bodies must guarantee the security of the information systems that they are using to provide the users with online services (for example, the payment of criminal fees for minor offences) and to correspond with them electronically. For such purpose, they must respect a general security referential, which defines the rules and best practices to be followed, and terms such as certification, official approval or security audits (www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/). This general referential indirectly applies to the service providers used by the administration, including for cloud computing services.

In this context, the ANSSI adopted a referential of specific requirements for cloud computing service providers called 'SecNumCloud'. The last version of this document was published on 11 June 2018 (www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf). It covers the various types of cloud computing services: the software delivered as online services, the infrastructures (offices and data centres) and the operating, management and operational procedures of the providers. This label is considered as much more demanding than others such as ISO 27000. So far, one provider is a 'qualified service provider' for cloud computing services under this referential (Oodrive). As at July 2019, six other certification applications were in progress (https://www.ssi.gouv.fr/liste-produits-et-services-qualifies).

Heritage Code (public sector)

The Heritage Code defines the legal regime for the archives of the state and other public bodies in general. It sets obligations for their safekeeping, which may only be outsourced if the provider is approved and if the archives are kept on French territory (article R212-23).

French Public Health Code (health sector)

Article L1111-8 of the French Public Health Code requires that health data hosting providers implement specific safeguards, fulfil certain commitments and be certified. Failure to meet the requirements defined by the public health agency (ASIP Santé) is sanctioned by a fine of €45,000 (and three years' imprisonment (article L1115-1)).

Order dated 3 November 2014 of the French Finance Ministry relating to the internal control of companies in the banking sector and others (financial sector)

The French Supervisory and Regulatory Control Body (ACPR), which is in charge of preserving the stability of the financial system and protecting the customers, insurance policyholders, members and beneficiaries of the businesses under its control, clarified in 2013 that cloud computing services should comply with the rules governing the outsourcing of banking activities. These rules are now set forth in an Order of 3 November 2014. Among other requirements, this text provides that the relevant businesses must remain able to terminate at any time the outsourcing services they use without this affecting the continuity or quality of the services they provide.

More recently, the European Banking Authority issued 'Recommendations on outsourcing to cloud service providers' which address five key areas: the security of data and systems, the location of data and data processing, access and audit rights, chain sub-processing, and contingency plans and exit strategies (www.eba.europa.eu). These recommendations must be applied by the national authorities (eg, the ACPR) to the relevant businesses.

Inter-professional Agreement dated 3 October 2016 concerning the obligation to seek continued exploitation relating to cinematographic and audio-visual works (cinema sector).

In the cinema industry, a trade agreement provides for the film producers' duty to ensure the conservation of the works used to create movies, so as to guarantee that such works are recorded in digital formats that enable their availability online. This agreement has been made mandatory by government decree. In furtherance thereof, a trade association, the Technical Superior Board of Image and Sound, has issued technical recommendations concerning, among others, the material conditions for the conservation of works under the contracts concluded with service providers (www.cst.fr: CST-RT043-2017-12-18-12h02.pdf).

Insolvency laws

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

The French Commercial Code provides the rules applicable to the insolvency of companies. No specific provision applies to cloud computing service providers, even though the consequences of their insolvency could be severe on consumers and professionals alike.

Therefore, appropriate precautions against the loss of data due to such situations should be incorporated into the contractual provisions governing the services, particularly with regard to reversibility and pricing.

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.

The processing of personal data is subject to the GDPR of 27 April 2016. This text has been supplemented by national legislation (Ordonnance No. 2018-1125 of 12 December 2018 amending the Law No. 78-17 of 6 January 1978 on information technology, files and freedoms; Decree No. 2019-536 of 29 May 2019). The main data protection rules applicable to cloud computing services delivered in France are the same as in the other EU member states (which was the main reason for enacting a regulation under EU legislation). The following aspects may be noteworthy.

Data controller and data processor

In most cases, a cloud computing service provider will be considered as a 'data processor' (ie, as acting pursuant to and under the instructions of its client). The client will, in turn, be considered as the 'data controller' (ie, the party who determines the purposes and means of the data processing (GDPR, articles 4 and 28)).

Consequently, obligations pertaining to the relations with the concerned individuals ('data subjects') will continue prima facie to be assumed by the clients. This concerns, in particular, the requirement for the individuals' consent to the data processing; the duty to minimise

data collection to the types of data actually necessary; the duty to keep data up-to-date and for no longer than is necessary to fulfil the processing's purposes; the duty to ensure the security and confidentiality of the data against unauthorised or unlawful processing and against accidental loss, destruction or damage; the duty to respond to individuals' requests to correct, delete or transfer their data. On the other hand, insofar as they qualify as data processors, the service providers will be responsible mainly for the implementation of technical and organisational measures that ensure a level of security appropriate to the risks inherent to the data processing. Their obligations in this respect are detailed in question 19.

However, it must be emphasised that the GDPR expressly provides that the parties to a service contract may be considered as joint data controllers. In a market where certain types of cloud computing services are dominated by a few service providers, this clarification is intended to correct some imbalances inherent in adhesion contracts (see question 16).

Cross-border transfers

Under the GDPR, personal data may be transferred out of the EU only if adequate safeguards are implemented (article 44 et seq). This requirement also applies to cloud services directed at individuals residing in France but based on servers located outside the EU. Thus, the use of servers outside the EU is not prohibited per se, but it is regulated, with a view to granting individuals the same protection as within the EU. Furthermore, data is considered as being transferred to any given country as soon as access to such data is technically possible from such country. To locate the servers within the EU is, therefore, not sufficient to determine that data is not processed abroad and that a cross-border transfer is not taking place. Similarly, one may not consider that cloud services based on servers located in France are per se compliant, if the data controller does not ensure that 'sufficient guarantees' are provided by the cloud computing service provider.

Individuals' rights

In the event that the cloud computing service provider proposes to transfer personal data out of the EU, the data subjects must be informed not only that their personal data is processed by a data processor, but also that it is transferred outside the EU (GDPR, articles 13 and 14). In the event that the service provider is faced with a security breach, it must notify its client without delay and notify the persons whose data is involved. Also, the service provider will have to enable 'data portability' (ie, to enable its client to deliver the personal data upon request to the relevant data subjects, in a structured, commonly used and machine-readable format), and to transmit such data to another controller without any impediment (article 20).

The French data protection authority (CNIL) issued recommendations on cloud computing services in 2012 (www.cnil.fr: Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a des_services_de_Cloud.pdf). Although they need to be updated with the GDPR, these recommendations provide useful guidance on how to implement data protection in agreements.

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)?

Cloud computing offerings are characterised by a multitude of contract documents, which for most providers include, as a minimum:

- the general conditions;
- the conditions specific to the given service;
- a service-level agreement defining the key performance indicators and the quality and service level commitments;
- a data processing agreement or privacy policy defining the commitments and exclusions relating to personal data protection; and
- an 'acceptable use policy' specifying the lawful conditions for use of the service.

These documents are multiplied according to the requirements of each service, which results in the service providers presenting comprehensive and complex catalogues.

These standard documents are generally recent and are regularly updated. The entry into force of the GDPR on 25 May 2018 (see questions 15 and 19) requires significant adaptations, just like Order No. 2016-131 dated 10 February 2016 reforming the French law of contracts (with its ratification Act No. 2018-287 of 20 April 2018). Among various provisions aimed at sustaining contractual justice, the new contract law indeed provides that a contract that includes a set of non-negotiable clauses that are predefined by one of the parties constitutes an 'adhesion contract'.

In such a contract, a clause will be considered as non-existent where it causes a significant imbalance between the parties' rights and obligations. In the event of any doubt, an adhesion contract will be interpreted against the party that proposed the contract. Comparisons may be made with the abusive clauses regime which protects consumers in business-to-consumer contracts.

This new statutory regime may help alleviate certain one-sided provisions that thrive in standard cloud computing contracts and help introduce more balance in favour of customers, as will be seen in the following questions. Such a reassessment remains contingent, however, on the application of French law to the contract.

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?

Governing law and dispute resolution

Standard contracts always include a clause defining the applicable law and which court has jurisdiction. The service providers thereby submit their contracts to the law and courts of the state where their establishment is located. Often, they have an establishment in the European Union. In France, their contracts are therefore often subject to the law and jurisdiction of a member state of the EU.

Enforceability

The public cloud contracts do not offer much opportunity for negotiation. As a consequence, the enforceability of their provisions is not necessarily guaranteed under the law – for example, in regard to the consent given by the client on standard documents that prove to be inaccessible or that allegedly should evolve without his or her express approval.

The clients frequently request the right to audit how the services are carried out in order to verify the services compliance with the provider's commitments, in particular with regard to security. The GDPR provides for this right (article 28.3). Since, in practice, it is difficult and costly for the providers to continuously accommodate the auditors sent by the clients, the providers try to obtain certifications (eg, ISO 27000) and propose in their clauses to communicate their own audit reports in order to limit the need for the clients to carry out additional verifications.

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?

Flexibility

Flexibility is a key component of cloud computing contracts. The hosting services are generally invoiced on the basis of the resources granted to the client (eg, number of servers, CPUs, etc). Agreements usually offer the possibility to cease both use and payment of the resources at short notice. Clients may add services or increase their capacity through online portals without the need to sign contract amendments. Flexibility is also reflected in the contract duration, which may run by the month, thereby enabling the clients to include the costs in their operating expenses.

Acceptable use

A cloud computing contract generally includes clauses to define limitations of use of the service by the client and its employees (often grouped together in an 'acceptable use policy' appendix). Usual clauses prohibit:

- use beyond the client's internal business purposes;
- use violating third parties' intellectual property rights; and
- use for unlawful purposes, including to harass, defame or abuse third parties or to post obscene, violent or discriminatory content.

Although cloud computing services are often presented as being 'content neutral' and customers' data considered as protected by confidentiality, service providers reserve the right to enquire about suspicious use and to suspend access and to put an end to the service in the event whereby the client's data would appear to infringe upon the restrictions of use.

This reflects the increasingly stringent legal constraints to ensure that the internet players assume responsibility for the online content. For example, an employer must ensure that his or her internet access is not used by his or her employees to replicate or disseminate works protected by copyright (article 336-3 of the French Intellectual Property Code). This indirectly concerns the cloud computing service provider working for such employer.

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?

Confidentiality

The terms and conditions covering data and confidentiality in contracts subject to French law are similar to those found under other laws. By way of principle, cloud service providers undertake to protect the confidentiality of their clients' data. Access to such data is granted to their employees on a 'need-to-know-only' basis, insofar as required to deliver the services. Reference is often made to the employees' individual confidentiality commitment, which is required by the GDPR and will usually be provided for in labour contracts.

Unlike pure players, which focus their services on the provision of infrastructure or storage for clients' data and purport to be 'content agnostic', cloud service providers that provide software or other value added services often seek to gain a right to access and use customers' data with a view to building up 'big data' pools on their own. This will often be provided for through a clause enabling such use for the purpose of 'improving the services' or 'customising the customer's experience' of the service. Such purpose often covers targeted advertising.

In such circumstances, the confidentiality of clients' and individuals' data may be jeopardised. For example, in July 2016, the CNIL noticed that through the processing of users' data for Windows applications, Microsoft was obtaining information on all the applications downloaded and installed by the users as well as the time spent on each application, which was not necessary for providing the service. Furthermore, an advert ID was activated by default upon the installation of Windows 10, which enabled Microsoft to follow the user's browsing and to target the advertisements without the latter's prior consent. The corrections requested by the CNIL have since been made.

The confidentiality clauses also show their limits in front of legislation requiring the service providers to disclose users' data to their governmental authorities (eg, US Patriot Act and US Cloud Act). The GDPR meets this type of situation by requesting the providers to inform their clients beforehand on the legal obligations of communication that may apply and prohibit them from deferring to such requests if they are not based on a mutual legal assistance treaty or similar (GDPR, articles 28 and 48). To date, many clauses still need to be more specific on this issue.

Location of data and data processing

In this context, numerous services attempt to reassure clients by guaranteeing that the data will only be stored in their country of residence or elsewhere in the European Union. The clauses often provide that the client may or will be informed of any modification of the location or country of storage. Under the GDPR, the client's approval as data controller is required and must be given prior to such modifications. It must be restated that this consent is necessary for any kind of data transfer, however: this is not limited to the country where data is stored, but applies to all the countries in which access to the data is possible.

When the cloud computing provider acts solely as a data processor within the meaning of the GDPR (ie, does not define the aims and means of the data processing), the GDPR requires that its agreement with the data controller specifically define certain obligations (article 28), including for the provider:

- to process the client's personal data only on documented instructions from the controller, including with regard to cross-border transfers;
- to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include, as appropriate:
  - pseudonymisation and data encryption;
  - ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - maintaining the provider's ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
  - regularly testing and evaluating the effectiveness of the measures taken to ensure the security of the processing; and
- to engage sub-processors only with the client's prior authorisation and to have them subject to the same data protection requirements.

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?

Service levels and warranties

The stakes of the cloud computing contracts reside in the characterisation of the providers' obligations, with the well-known contrast under French law between the best-efforts obligation (for example, 'the service provider will use reasonable efforts to provide the services with the level of diligence and competence that could reasonably be expected for services of a such nature and of a complexity substantially similar to that of the services') and the performance obligation ('the provider guarantees the continuous availability of the service during business hours'). In general, the service provider contracts avoid guaranteeing

the availability and performance of their services or formulate service levels and exceptions (eg, planned maintenance, minimum downtime, etc) that enable a large degree of latitude.

The challenge for the cloud computing service providers is indeed to offer a service that is ready to use and works 'end-to-end', whereas, in practice, they do not master the production chain which begins at their servers through to their clients' workstations. The cloud providers are rarely telecom operators and do not operate the internet connections. Furthermore, SaaS providers rarely own their data centres and, accordingly, are dependent on hosting providers. The IaaS and PaaS providers are, in practice, the ones actually in control of the service levels concerning the availability, reliability and quality of the cloud computing services. For these reasons, the service-level agreements are often sanctioned by a notion of 'service credit', which allegedly compensates for a default in the service with an extension of its duration.

Liability

As the cloud computing services market is dominated by a few global infrastructure and platform providers, the liability clauses significantly restrict their indemnification commitments. The liability cap in the event of a loss of client data is frequently fixed at the level of the monthly instalment paid by the client although, under French law, any clause that nullifies the debtor's essential obligation will be considered void (New French Civil Code, article 1170).

With regard to the damages applicable in the event of non-compliance with the GDPR, a client may request a guarantee from its cloud computing provider insofar as the latter acted as a 'sub-contractor' and failed to comply with his or her regulatory obligations specific to sub-contractors or with the instructions received from his or her client in this regard (article 82).

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?

The terms and conditions governing intellectual property rights (IPRs) in contracts subject to French law are similar to those found in contracts subject to other laws: typically, each party remains the sole rights holder on all the IPRs applicable to its materials, that is, the software programs it provides via the services, as regards the service provider, and the data and third-party software programs stored in the cloud and used by the client, as regards the latter.

Licence rights are granted by each party to the other insofar as necessary for the other party's supply or use of the services, as applicable. Customisation is not typical of standard services such as IaaS and PaaS, but should this arise in the form of copyrighted work (eg, specific developments), the service provider will, in general, grant licence rights and avoid any IPR assignment to the client.

In the same vein, cloud computing contracts require each party to indemnify the other against any infringement claims from third parties. Often, the service providers' standard terms and conditions will entitle them to terminate their services in cases where the client is found to infringe third-party rights.

Typical terms covering termination

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

Term and termination

Cloud computing contracts are usually entered into for a fixed term, typically from one month to one year. This duration may be extended or renewed, expressly or tacitly, but the client does not necessarily benefit from a renewal guarantee. In this regard, the new French law of contracts sets forth that no party may impose the renewal of a contract (Civil Code, article 1212). Therefore, attention should be paid to the notice period and the terms of renewal.

More traditionally, the termination clauses provide an exit right for each party in the event of non-compliance by the other party. In non-negotiated contracts, it will be difficult for the client to use such clauses as a credible threat against non-compliance relating to the service level or quality of the service provision.

Reversibility

At the end of a cloud computing service, the client must recuperate its assets (ie, programs and data). As they are standard , the reversibility of the IaaS and PaaS services does not require the transfer of know-how and knowledge specific to the provider. Nonetheless, assistance from the latter is often available as an option.

However, the specificities of a program implemented on the cloud (eg, specific developments and settings according to the client's business rules, etc) and data formats set up by the provider (sometimes proprietary or using variants of the existing standards) may result in a lockout of the client. The reproduction of the existing solution or the system's output available for data migration may also pose a problem. Despite their multitude, contractual documents are often lacking specifications and commitments in this regard (see question 26).

The entry into force of the GDPR should encourage the emergence of more adapted stipulations, as this text obliges data controllers to enable data portability (see question 15). The clients could use this as guidance to address the practical issues raised by reversibility situations. In any case, healthy competition between several providers and services remains the most effective tool in order to avoid harmful dependence.

Employment law considerations

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

In cases where activities are transferred from one company to another, the Labour Code will govern the transfer of employment contracts (articles L1224-1 and L1224-2). A contract for the supply of private cloud computing services may be part of or may follow such a transfer of personnel from the client to the service provider. However, it will usually rather be considered as an outsourcing contract. In general, cloud computing contracts per se are indeed not understood to involve a transfer of personnel by the client. This is reflected in the statutory definitions of cloud computing (see questions 8 and 9), which do not refer to such an element.

TAXATION

Applicable tax rules

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

The cloud computing service providers are currently subject solely to the standard corporate tax, at 33.33 per cent. This rate should progressively diminish to reach 25 per cent in 2022.

Nonetheless, as cloud computing providers may exercise an activity in a country without any human and material resources and, accordingly, may be considered as not having a 'fixed establishment' in the country, French corporate tax does not apply equally to all the providers of the sector that sell services in France. The judgment rejecting the taxation of Google Ireland Limited imposed by the French tax authorities is a relevant example (Paris Administrative Court, *Google*, 12 July 2017).

This situation should evolve in the coming years with the progressive modification of the applicable international rules, including the redefinition of the notion of fixed establishment and the creation of a tax specific to cross-border digital services. Pending the adoption of such a tax treaty by the OECD members, the French government has decided to impose a tax on digital services providers with digital revenues in excess of €750 million internationally and €25 million nationally, based on their turnover and amounting to 3 per cent thereof. In the summer of 2019, the French government declared at the G-7 meeting that France will adhere to the new tax regime to be defined by the OECD in respect of digital activities, once the member states converge on a global consensus, and that the government will subsequently unwind the French digital tax and refund the overpaid amount to the tech companies, if any.

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.

The French General Tax Code classifies the cloud computing services in the category of 'electronic service provisions' (appendix 3, article 98 C, c). These services are subject to the standard VAT rate (20 per cent).

The application of VAT to cloud computing services is complex, as the location of the provider's taxation varies depending on whether the client is itself liable to charge VAT (the location is then his or her establishment in France) or not (the location of taxation is the place where the beneficiary of the services is established, at his or her domicile or habitual residence, including abroad) (article 259 et seq).

Whether they are established in the EU or not, the service providers may follow a special tax regime for clients that are not VAT collectors, which provides a mini one-stop-shop mechanism to liquidate VAT owed in the various member states of the EU.

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.

Paris Administrative Court, Google, 12 July 2017

Even though the French administration focused on the search engine activity and the income gained from the advertising services invoiced by Google to its French clients (AdWords), the discharge by the Administrative Court of the tax reassessments requested in terms of corporate tax, withholding tax, VAT and various contributions could also apply to cloud computing services (see question 25). This litigation shows the significant challenges inherent in the business model of international cloud computing service providers (http://paris.tribunal-administratif.fr/Actualites-du-Tribunal/Communiques-de-presse/La-societe-irlandaise-Google-Ireland-Limited-GIL-n-est-pas-imposable-en-France-sur-la-periode-de-2005-a-2010).

Versailles Court of Appeal, 19 May 2015, No. 14/08016

In the context of an objection procedure against the registration of a trademark 'CLOUD CUBE', the Versailles Court of Appeal judged that the term 'CLOUD' can be readily understood by the consumer as referring to the expression 'cloud computing' and, consequently, that it already shows the destination of a certain number of products and services. Accordingly, it cannot be considered to be distinctive. The dismissal for the registration of the trademark was being requested by the holder of a prior trademark '+ LE CUBE' and was upheld by the court.

FERAL-SCHUHL / SAINTE-MARIE
law firm

Olivier de Courcel
odecourcel@feral-avocats.com

Stéphanie Foulgoc
sfoulgoc@feral-avocats.com

24, rue Erlanger
75016 Paris
France
Tel: +33 1 70 71 22 00
Fax: +33 1 70 71 22 22
www.feral-avocats.com

ARSENE
TAXAND NETWORK

Alain Recoules
alain.recoules@arsene-taxand.com

32, Rue de Monceau
75008 Paris
France
Tel: +33 1 70 38 88 00
Fax : +33 1 70 38 88 10
www.arsene-taxand.com

CNIL, Google LLC, 21 January 2019, No. SAN - 2019-001

Upon verification of the data processing relating to the use of the Android operating system on mobile phones, including the creation of a Google account, the CNIL observed that the information on the processing of advertising customisation was excessively disseminated in separate documents and, therefore, not easily accessible to users. As a consequence, the regulatory authority determined that the consent on which Google relies for this processing is not obtained validly with regard to the law of 6 January 1978 on data processing and freedoms and the GDPR. In light of the data processing operations and the number of persons concerned, the CNIL considered that the lack of transparency as well as the lack of valid consent constituted substantial breaches of privacy and run counter to the legitimate aspirations of individuals wishing to retain control of their data. It ordered Google LLC to pay a fine of €50 million.

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?

Although the pressure of software publishers on their customers to shift their office automation and other software applications to the cloud is maximal (eg, Office365 and OneDrive) and raises questions about the concentration of the cloud computing market onto a few global players, a yearly enquiry by CyberArk's Global Advanced Threat Landscape Report shows that privileged access is the biggest cloud security issue: 'The risks created by the lack of clarity about who is responsible for security in the cloud are compounded by a general failure by organisations to secure privileged access in these environments', according to Adam Bosnian, executive vice president, global business development. Only 47 per cent of organisations reportedly currently have an access management and security strategy in place for cloud and workload infrastructure (https://www.cyberark.com/press/global-advanced-threat-landscape-2019-focus-on-cloud/).

Germany

Viola Bensinger and Laura Zentner
Greenberg Traurig Germany, LLP

MARKET OVERVIEW

Kinds of transaction

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

All types and service models of cloud computing are used in Germany. In the private sector, and both in B2B and B2C relationships, the use of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (SaaS), including storage, is common. Due to security concerns, companies prefer private cloud computing rather than a public cloud. However, according to the most recent 'Cloud-Monitor' – a study by German industry association Bitkom – public cloud models are gaining ground, with more and more companies willing to store information in public clouds. Nevertheless, the most important factor for companies in selecting a cloud provider is compliance with the EU General Data Protection Regulation (GDPR).

German government agencies also increasingly rely on the 'federal cloud', a light house project established in 2016 and operated by the Federal Information Technology Centre (ITZ Bund). The federal cloud offers all service models including IaaS (eg, Federal Cloud Server), PaaS (eg, Federal Cloud Development Environment) as well as SaaS (eg, Federal Cloud Runtime Environment) and is to become the standard for federal authorities. It ensures that all data are stored on servers within Germany. In addition, and subject to certain requirements, federal and regional public authorities also use cloud services offered by private German and global providers.

Active global providers

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

Apart from the three most prominent cloud service providers, Amazon (Amazon Web Services), Microsoft (Azure) and Google (Google Cloud Platform), many other global enterprises offer cloud services in Germany. Especially IBM, Alibaba, Deutsche Telekom, Oracle, Exoscale and Profitbricks hold an appreciable position on the German cloud computing market.

The German business community is increasingly opening up to both existing and new cloud services. The market is likely to remain attractive and profitable for the industry's global players.

Active local providers

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

Even though two-thirds of all cloud users rely on global providers, there is a distinctive market in Germany for local cloud providers offering their own variety of services. These smaller players (eg, Strato) offer secure and innovative cloud solutions, and often specialise in a particular type of cloud solution or service.

Market size

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

The German cloud computing market offers diverse solutions and services, and is fast-expanding. Cloud services are accepted and used by a growing number of companies, including numerous small and medium-sized enterprises (SMEs). Also, Microsoft is reported to reintroduce a new version of its German cloud after previously having discontinued this service for German customers in September 2018. According to statistical reports published by Statista, currently the German market's volume is €4.5 billion for SaaS, €421 million for PaaS, and €705 million for IaaS. Total turnover for the (B2B) cloud computing sector is forecast to be €22.5 billion in 2020.

Bitkom's 'Cloud Monitor 2019' also evidences that cloud computing in Germany continues to grow. In 2018, three out of four companies (73 per cent) used cloud computing services, compared to two-thirds (66 per cent) in 2017. A further 19 per cent of the enterprises surveyed intend to use a cloud in the future. For only 8 per cent of enterprises, cloud services are not an option. Remaining concerns, especially of smaller enterprises, are data protection or integration issues, and fear of losing control of the cloud computing service.

Impact studies

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

Several studies on cloud computing in Germany are publicly available (eg, Bitkom's annual Cloud Monitor, see question 4) or studies by the Federal Office for Information Security (BSI). In addition to market figures, trends and the overall attitude of companies as regards cloud computing, such studies also provide more specific insight, such as the decisive factors for cloud users in Germany and of the remaining challenges of cloud computing for German enterprises.

Recently, the European Commission launched a study to assess current and future energy consumption and state-of-the-art cloud computing services in Europe. The study aims to develop recommendations for energy-efficient cloud computing, particularly regarding future research and development, green public procurement and market policies. The study is expected to be finished in early 2020.

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?

There is no government policy generally promoting establishment of cloud computing centres in Germany. Rather, the programmes in place encourage cloud providers to meet certain quality and security standards, thereby improving their market position.

One example is the Trusted Cloud project, originally a governmental subsidy programme that today is led by a non-profit organisation. The project provides certification (Trusted Cloud Label) and a marketplace for 'trusted' cloud services through the Trusted Cloud Portal. The criteria for certification include IT and data security, quality and transparency, data protection and service contracts (details on www.trusted-cloud.de). The portal aims at both cloud users and providers; however, primarily it targets SMEs.

The government agency BSI offers another standard, 'Cloud Computing Compliance Controls Catalogue' (C5), which primarily addresses large and medium-sized enterprises and focuses on IT security and transparency. C5 is more detailed with higher thresholds than Trusted Cloud, and C5 certification is deemed to also evidence that the requirements for TOMs under GDPR are met.

The German federal government also provides for its own 'federal cloud' infrastructure (see question 1), which currently is only available to federal institutions.

Incentives

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

There are no specific tax or custom incentives or other government subsidies for cloud computing in Germany.

However, both the federal government and the governments of the German federal states offer a wide variety of state aid programmes to promote digitisation of the European or German economy. In particular, support is provided to SMEs for digitisation projects, but usually only for the users of cloud infrastructures (and not for providers). The platform www.foerderdatenbank.de provides a comprehensive overview of available subsidies.

LEGISLATION AND REGULATION

Recognition of concept

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

There is no legal framework in Germany specifically for cloud computing. Therefore, cloud computing services are subject to general laws such as the German Civil Code, the German Commercial Code, the GDPR, the German Copyright Act or the rules against unfair competition.

Governing legislation

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

The only specific legislation governing cloud computing is German IT security law (BSIG), which now also implements the EU NIS Directive. The BSIG imposes certain IT security obligations on providers of critical infrastructure.

Pursuant to section 2, paragraph 11 No. 3 BSIG, cloud computing qualifies as 'digital services' that enable 'access to a scalable and elastic pool of commonly usable computing resources'. Generally, cloud computing services do not fall under the definition of critical infrastructure of the BSIG and associated regulations (except for cloud services operated by state or federal administration, eg, the 'federal cloud'). However, non-governmental cloud services may qualify as critical infrastructure for the information technology and telecommunications sector in the future, and would then have to meet requirements under BSIG. Also, and more importantly, where a provider of a critical infrastructure uses a cloud service, it will try and contractually impose the legal requirements on the cloud provider.

BSIG stipulates various IT security requirements for providers of cloud services of a certain size, including the obligation to take adequate technical and organisational measures to maintain a level of IT security that minimises risks to the security of the network and information systems used for the service. Cloud providers that are subject to BSIG also must report to BSI all security incidents that have significant impact on the respective service.

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

A variety of German regulations and legislation may have indirect impact on cloud computing services. In addition to the general provisions of the German Civil and Commercial Codes and the rules against unfair competition, particular attention should be paid to the relevant data protection provisions of the GDPR and the German Data Protection Act. However, each cloud computing service may face specific issues depending on its business model and offerings.

Software made available via cloud computing may be subject to German copyright law. While software packages made available via cloud are usually used online without being copied to the user's device, the use may still qualify as an action that requires a licence (contrary to a mere copyright neutral enjoyment of a work).

The provisions of the German Telecommunications Act (TKG) may apply to cloud computing services only in exceptional cases (ie, if the service qualifies as a telecommunications service within the meaning of section 3, No. 24 TKG, eg, because it includes Voice-over-Internet-Protocol, video conferencing, instant messaging or email services). In this case, the service would be subject to strict rules of secrecy of telecommunications and obliged to register with the Federal Network Agency.

Breach of laws

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

Under German law, there is no general consequence applying to legal violations in the context of cloud computing. Depending on which provisions are violated, the following main types of consequences or sanctions must be considered.

If providers or customers do not comply with regulatory requirements, this may trigger administrative proceedings. This may, for example, result in investigations, conditions to be completed or even prohibition of the practice complained about, or, in exceptional cases, of the respective cloud service.

In the case of certain infringements, supervisory authorities may also impose administrative fines on cloud providers or users,

for example, in the area of data protection. According to the GDPR, fines of up to €20 million or 4 per cent of the worldwide turnover of the preceding financial year, whichever is higher, may be imposed on providers or customers who operate or use cloud computing services not in compliance with the requirements.

Certain particularly serious infringements may result in criminal liability. Currently, German law only holds individuals liable under criminal law (however this may change as it is being discussed to extend criminal liability to enterprises). For example, employees of the cloud provider may be liable to prosecution for certain forms of illegally tampering data. In addition, if a cloud provider is commissioned by persons subject to professional secrecy (eg doctors, attorneys, tax advisors), the provider's employees may also be liable if they disclose information protected by professional secrecy to third parties (section 203, paragraph 3 German Criminal Code).

If cloud providers violate certain regulations of unfair competition law, competitors or customers may claim injunctive relief or damages, or both. As far as consumer protection regulations are concerned, also consumer protection organisations are entitled to issue warnings against such cloud providers and to claim injunctive relief.

Consumer protection measures

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

German law provides for a range of consumer protection measures, of which the rules on distance selling (sections 312c et seq German Civil Code) have notable impact on cloud services. Among other obligations, providers are subject to extensive information requirements (eg on provider details, scope of services, total costs, warranty). Consumers also have a 14-day withdrawal right from the contract.

In addition, the provisions in sections 305 et seq German Civil Code on the use of standard terms and conditions restrict provider-friendly drafting, and prohibit surprising or unequitable terms, particularly in B2C contracts. Restrictions include controls on the exclusion and limitation of liability, dispute resolution clauses, venue and governing law, contractual penalties, or contract term. These provisions are mandatory law that, vis-à-vis customers residing in Germany, cannot be circumvented by choice of a different law.

Regulation (EU) No. 524/2013 on online dispute resolution for consumer disputes imposes further information obligations on providers.

Sector-specific legislation

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

There is no general cross-industry and cross-sector legislation for cloud computing in Germany. However, the BSI Act (BSIG) contains industry- and sector-specific IT security requirements for operators of critical infrastructure such as energy, telecommunications, insurance or health. If companies in these critical sectors use (or provide) digital services such as cloud computing, they may have to comply with increased requirements for technical and organisational measures to protect their IT systems, and to report significant IT security incidents to BSI. In 2017, BSI also published a Cloud Computing Compliance Controls Catalogue (C5; see also chapter 6) defining criteria for assessing IT security of cloud services. Based on international standards, C5 provides companies with a uniform and generally recognised framework for ensuring IT security in cloud computing.

In addition, companies in specific sectors need to comply with industry-specific legal requirements, for example:

- the German Banking Act, Payment Services Supervision Act, German Securities Trading Act, Investment Act regulate the financial sector;
- the Insurance Supervision Act applies to insurance companies;
- Companies in the energy sector are subject to the Electricity and Gas Supply Act; and
- the telecommunications sector is governed by the TKG.

Companies in the healthcare and legal sectors are subject to certain provisions of the German Criminal Code and rules of conduct.

The respective supervisory authorities usually issue guidelines to specify these sector-specific requirements. For example, federal financial supervisory authority BaFin provides detailed information on the legally compliant use of IT, including cloud computing, for the financial sector, particularly regarding IT security, contractual design and data protection. In the public sector, the resolutions of the Council of IT Officers (2015) and the IT Planning Council (2016) provide criteria for the use of cloud services by the federal administration (cloud services of private providers may only be used subordinately, and data may only be stored in Germany and may not be subject to disclosure or publication obligations, such as the US CLOUD Act).

Insolvency laws

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

As there is no specific insolvency law for providers of cloud computing or other IT services, the general German Insolvency Statute applies (if German insolvency law is applicable under conflict of laws rules).

For most insolvent companies an insolvency administrator will be appointed. The administrator is generally free to either continue to perform, or to refuse to perform, the ongoing obligations of the cloud computing contract.

If the customer of a cloud provider becomes insolvent, the administrator is likely to refuse performance of the contract and to cease payments, in which case the provider is entitled to cease provision of the services due to payment defaults. The administrator may also elect to continue the contract for a limited time if necessary (and feasible) for the administered company but then needs to pay for (future) services.

If the cloud provider files for insolvency, the administrator may choose to refuse performance (ie, stop the provision of services). In this case, customers should in most cases be entitled to claim separation of their stored data, and the migration or deletion of such data. The practical enforceability of such a claim may, however, depend on whether the insolvency estate has sufficient funds to operate the respective servers. If not, the administrator (or hardware provider) will switch off the servers and prevent further access to the customers' data. Should the cloud provider's administrator elect to continue the contract, the services will be available irrespective of the insolvency proceedings. Customers will then have to assess whether they have a contractual right to terminate the cloud computing contract, which remains enforceable in the provider's insolvency.

A contractual termination right in the event of the other party's insolvency is often unenforceable under German law.

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.

In Germany, any (automated) processing of personal data is governed by the GDPR and the supplementing provisions of the Federal Data Protection Act. If cloud solutions are used, login data and other content containing personal data are typically transferred to and processed

by the provider. Therefore, ensuring compliance with applicable data protection law is a crucial issue for cloud computing services.

GDPR applies to cloud providers and customers established in the EU/EEA, regardless of whether the processing of data takes place in the EU/EEA or the data pertains to EU/EEA residents. Providers established outside the EU/EEA may also be subject to GDPR, particularly if they address the German market or offer cloud services to individuals residing elsewhere in the EU/EEA. If they offer their services to corporate customers established in the EU/EEA, those customers will impose certain obligations under GDPR on cloud providers by means of a data processing agreement, standard contract clauses and similar instruments.

GDPR stipulates various requirements for the processing of personal data. If a provider or customer fails to comply with relevant requirements, fines of up to €20 million or 4 per cent of the worldwide turnover of the preceding financial year may be imposed, depending on the nature and severity of the infringement. In addition, the supervisory authority may carry out investigations including data protection audits, or order the respective entity to remedy the violation (eg, to change processes or even to cease using a particular service).

The following requirements are particularly relevant for cloud computing.

From a GDPR perspective, it is usually the cloud user who is deemed responsible controller deciding on the processing of personal data, while the cloud provider is deemed to process data on behalf of the user. To comply with GDPR, the parties must conclude a data processing agreement with certain minimum contents pursuant to article 28 GDPR. This includes provisions obligating the cloud provider to only process data per the customer's instructions, and to not use subcontractors without the customer's consent.

If cloud services are based on infrastructure located outside the EU/EEA, personal data are transferred to third countries. If there is no adequacy decision adopted by the EU Commission for the respective third country (eg, the United States), under GDPR the parties are required to ensure appropriate safeguards achieving an adequate level of protection. To that end, providers (and any subcontractors) and customers usually enter into EU standard contract clauses for processors. If the provider or subcontractor is located in the US, they can alternatively obtain certification under the EU–US Privacy Shield, which also establishes an adequate level of protection.

Cloud providers must also sufficiently evidence to have implemented appropriate technical and organisational measures (TOMs) for data processing, and to ensure protection of the rights of customers, employees, or other third parties.

To provide practical guidance on how to use cloud computing solutions in compliance with data protection law, German supervisory authorities have issued a joint guideline. This guideline 'Cloud-Computing Version 2.0', issued in 2014 by the Conference of Data Protection Commissioners of the Federal Government and the States, summarises the most important risks when processing data in clouds, requirements for the contractual set-up of cloud services, and recommendations for technical and organisational requirements. Since the guideline still refers to the legal situation before GDPR entered into force, an updated version is currently being drafted.

For cloud providers subject to US law, the obligations to disclose data under the US Cloud Act is particularly problematic. According to a statement of the European Data Protection Board, there is no valid legal basis for such data transfers to authorities in the US except in few exceptional cases. Furthermore, it is unclear whether customers also violate the GDPR, and therefore risk a fine, when using a US cloud provider.

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)?

As cloud services exist in various forms, their provision cannot uniformly be characterised as a specific type of contract under German law. There is also no consistent case law on this issue. While most cloud computing contracts will be a hybrid of different contract types, the following may serve as a guideline:

- IaaS: The provision of storage capacity usually qualifies as a lease contract, while the provision of computing power classifies as a service contract;
- PaaS: Access to infrastructure for development tends to be a lease contract; and
- SaaS: Such contract on providing software usually qualifies as a lease contract (or a loan contract if the SaaS service is free of charge).

However, accurately classifying a cloud computing contract will always depend on the individual circumstances. To minimise the considerable legal uncertainties, cloud computing contracts (both individual contracts and standard business terms) typically comprehensively describe the terms of use of the respective services as well as other relevant issues.

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?

According to article 3 of the Rome I Regulation (EC No. 593/2008), the parties in B2B cloud computing relationships are free to choose the governing law both in individual contracts or standard business terms. For German cloud providers, the choice of German law is usually non-negotiable, whereas large global providers regularly insist on the law of the country of their primary establishment.

The place of jurisdiction is typically chosen corresponding to the governing law. Agreements on enforceability or (other) cross-border issues, however, are uncommon in cloud contracts.

Arbitration clauses have become more common in cloud contracts, but still are not typical in Germany.

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?

If the cloud service is not free of charge, the cloud computing agreement usually provides for prices and payment modalities. In the case of IaaS and PaaS, providers often charge by time or volume of processed data, based either on actual usage (actual on-demand service) or on capacity held. SaaS are often billed at a fixed price per user or application, or based on actual usage (eg, per time). Additional services such as training or data migration are usually charged separately.

Price adjustment clauses in cloud computing contracts are quite common. In order for such clauses to be enforceable, the price increase may only be linked to comparable products pursuant to the German Price Clause Act. If the price adjustment is included in standard business terms, it must also meet the requirements in section 305 et seq

German Civil Code, particularly regarding transparency and adequacy or equity. Benchmarking clauses are probably more common.

Most cloud computing contracts include an acceptable use policy (AUP) which prohibits the use of the services for illegal activities (eg, infringing third-party intellectual property or other rights, sending email spam, or spreading viruses or other malware). Often, such AUP also prohibits excessive use. If users violate these rules, the cloud provider typically reserves the right to terminate the contract.

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?

Data protection is an indispensable issue in cloud computing because of the underlying processing of personal data and its inherently cross-border nature. Nevertheless, cloud framework agreements typically do not contain detailed data protection provisions in their main body, but refer to stipulations in annexes. Mostly, the customer and the cloud provider enter into a data processing agreement in accordance with article 28 GDPR. Where international data transfers take place, EU standard contract clauses are typically concluded and added as another annex.

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?

As the contractual relationship is often based on the cloud provider's terms and conditions, their liability is typically excluded as far as legally permitted, and capped at a maximum amount either per event of damage or for all claims arising from the contract.

However, according to German law governing standard business terms, standard terms may not limit liability for damage to life and health and for damage caused by gross negligence or wilful misconduct. To enforceably further limit or exclude the provider's liability, the liability clause needs to be individually negotiated.

Most cloud contracts include specific Service Level Agreements (SLAs) containing performance obligations, obligations regarding the availability of service or timely response of a helpdesk, etc. The customer will typically have to accept the provider's standard SLAs. While SLAs usually contain sanctions such as penalties or price reductions for failure to meet the stipulated standard, such penalties are often limited to fairly low amounts.

Further, a cloud contract should contain warranties regarding business continuity and disaster recovery.

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?

Typically, the provider grants to the customer a non-exclusive, non-transferable licence to use the provider's platform and – for example, for SaaS services – the provider's access or other software. The provider usually warrants to hold all necessary rights or licences to provide the services to the customer. The provider may further agree to defend and hold harmless the customer from any claims made against it by a third party due to an alleged infringement of IPR by the cloud service. However, such indemnification by the provider is not typical unless the customer has considerable leverage.

The customer may not modify the provider's software or use it in any unauthorised way, and has to impose any obligations and usage restrictions under the cloud computing contract on their customers. The customer will need to warrant that it holds all necessary rights to content stored in the cloud, and that the storage, use or transfer of the contents does not violate applicable laws or third-party right. The customer must also hold harmless and indemnify the provider from and against any third-party claims (including reasonable legal costs) made owing to unlawful actions or a breach of warranty by the customer.

The cloud provider regularly reserves the right to suspend provision of service, or even terminate the contract, if there is reasonable evidence of a violation of third-party rights or other unlawful use of the service by the customer (or any of its customers). The provider will sometimes also reserve the right to perform licence audits, and oblige customers (and their customers) to cooperate in such audits.

Also, for any breach of IPR warranties or obligations, the (contractual and/or statutory) general provisions on liability and on the remedies for breach of contract apply, including injunction of the violation and payment of damages.

Typical terms covering termination

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

Cloud computing contracts can be entered into for an unlimited contract term or for a fixed term, (typically for one or two years). However, usually any fixed term will be extended automatically if the contract is not terminated by one of the parties.

Any cloud services contract may further usually be extraordinarily terminated without notice for good cause. The conditions for extraordinary termination as well as circumstances establishing a 'good cause' are usually specified in cloud computing contracts. They commonly stipulate a right of extraordinary termination in the event of serious and repeated breaches of duty, such as major failures of the cloud service or significant payment defaults by the customer.

It is highly recommended to provide for an exit management. Otherwise, there is a risk that the cloud services will cease to be available to the customer immediately after the contract is terminated. As part of the exit management, the cloud provider is typically obliged to continue to provide services for a specified period after termination of the contract, and to support the user in transitioning the cloud services (and migrating data) to a new provider's (or the user's own) systems.

Employment law considerations

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

The introduction of cloud computing services by a company may be subject to participation rights of third parties under German employment law.

If a data protection officer has been appointed by the company, they must be informed prior to the introduction of cloud computing applications qualifying under article 38 GDPR and sections 6 and 38 of the Federal Data Protection Act.

If a works council exists in a company of cloud computing, it must be informed about the introduction at the preliminary planning stage. The works council also has a right of co-determination with respect to the introduction and use of technical equipment intended to monitor the behaviour or performance of employees, which is why the introduction of cloud computing services, owing to its technical possibilities, may require prior consent of the work council.

While unlikely, the introduction of cloud computing may qualify as a change of business if it leads to extensive changes in the

company's organisation or work processes, or triggers a major reduction in personnel. In this case, a reconciliation of interest procedure with the works council would have to be conducted, as well as a social plan concluded.

TAXATION

Applicable tax rules

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

Companies established in Germany are subject to income tax and trade tax (regarding VAT see question 25). Any individual or corporation starting a business in Germany is obligated to notify the responsible tax office before commencing business.

Income tax for individuals is governed by the German Income Tax Act and for corporations by the German Corporate Income Tax Act. Partnerships as such are not subject to income tax but treated as transparent and the profit shares are to be taxed by its partners. For individuals the tax rates vary from 14 per cent to 45 per cent. For corporations the tax is 15 per cent. In addition, there is a 'solidarity surcharge' of 5.5 per cent on the amount of income tax due.

Businesses (and partnerships) are also subject to trade tax. The basis for trade tax is the taxable profit for income tax purposes with certain additions and reductions. The tax rate depends on the place of establishment, and generally varies from 7 per cent to 18 per cent.

In addition, companies may be subject to withholding obligations. The most important withholding taxes for cloud computing providers are for the salaries of its employees (wage tax) and on licence fees (at a rate of 15 per cent) if paid to recipients outside Germany.

Foreign cloud computing companies providing services to customers in Germany are not subject to income tax or trade tax unless they maintain a permanent establishment in Germany. While the use of storage capacity on computers located in Germany as such is not considered to create a permanent establishment, maintaining (owned or rented) computers in a designated area of a building may qualify as permanent establishment and trigger income and trade tax liability. The fees paid for cloud computing services are generally not qualified as licence fees, and therefore not subject to withholding tax if paid by German customers to foreign cloud providers.

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.

Regarding VAT on cloud computing services supplied from outside of Germany to customers in Germany, there is a distinction between services rendered to VAT payers and services rendered to consumers.

For B2C transactions, cloud computing services qualify as electronic services, which are deemed to be supplied and subject to VAT at the place of the customer's residency or establishment. Hence the provider is liable for VAT, at a standard rate of 19 per cent.

For B2B transactions, although the service is deemed to be performed and subject to VAT at the place of the customer's establishment, not the supplier but the customer is liable for the tax (reverse charge mechanism).

The fact that the customer is a business must be evidenced by providing a valid VAT identification number.

Foreign cloud computing companies rendering only electronic services to consumers in Germany may claim any VAT incurred in Germany under the refund procedure.

GT GreenbergTraurig

Viola Bensinger
viola.bensinger@gtlaw.com

Laura Zentner
laura.zentner@gtlaw.com

Kollhoff-Tower
Potsdamer Platz 1
10785 Berlin
Germany
Tel: +49 30 700 171 100
www.gtlaw.com

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.

If cloud computing takes place between two German parties, and only local facilities are used for the service, there are hardly any tax differences compared to other commercial services.

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.

In the past three years, there has not been notable German case law, nor have there been commercial, private, administrative or regulatory determinations in Germany, directly involving cloud computing as a business model.

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?

From a purely legal perspective, and leaving business considerations aside, the main challenges for both providers and users of cloud services certainly are security, meeting legal and industry security requirements as well as balancing effective and customer-friendly workflows against proper security safeguards. While there currently are no cloud-specific legislative initiatives, etc, there are several envisaged changes that will certainly affect cloud providers, such as the planned revision of the EU product liability directive (and its implementation into national laws).

India

Samuel Mani and Rosa Thomas
Mani Chengappa & Mathur

MARKET OVERVIEW

Kinds of transaction

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

The Indian cloud computing market is a very vibrant market, and there are all varieties of cloud computing transactions taking place, in consonance with newer concepts as well, such as machine learning, edge computing and anything-as-a-service (XaaS). The private sector is leading the way, but the central government and state governments are also actively considering and implementing various cloud-based computing initiatives, in addition to partnering with private players to set up necessary infrastructure.

Active global providers

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

All of the major global cloud providers are active in India. Amazon and Microsoft are the leaders with their AWS and Azure offerings respectively, while Digital Ocean, Google, Cisco and IBM are also very active.

Active local providers

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

There are a host of smaller cloud providers in India. Given the nature of cloud computing, it is somewhat difficult to identify India-based and India-centric cloud service providers. Some of the cloud providers outside of the large global players that are commonly referred to in computing circles are NetMagic, BlueHost, HostingRaja and SoftLayer. They provide numerous services, which include web hosting, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), data security, fault tolerance, and disaster recovery. India's burgeoning technology product ecosystem is largely cloud-centric. Notable examples that have a significant Indian heritage include Zoho, Freshdesk, Freshworks and CtrlS.

Market size

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

The Indian cloud computing market is well established. India's small and medium-sized enterprises are actively migrating to cloud-based applications and large enterprises are also following suit. As a case in point, the Reserve Bank of India (RBI) recently granted more than 20 new banking licences to banks with various target markets. These new banks are very actively leveraging cloud-based infrastructure and applications, including mission critical applications such as core banking solutions. According to a report by Gartner, and according to NASSCOM's report 'Cloud – Next Wave of Growth in India' (www.nasscom.in/knowledge-center/publications/nasscom-cloud-next-wave-growth-india-2019), the current estimated spending as of 2018 on cloud services in India, is estimated at US$2.5 billion. This accounts for 6 per cent of India's expenditure on information technology. This is further expected to grow at 30 per cent per annum, to reach US$7.2 billion in 2022, which is nearly a threefold increase. The growth rate of the Indian public cloud market is the second highest growth rate globally, after China (www.gartner.com/newsroom/id/3874299). This shows that India is a critical growth market for all types of cloud computing players.

Impact studies

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

There are numerous studies that are carried out in the cloud computing ecosystem in India. Reports and studies are published by leading researchers such as Gartner, Forrester, IDC and Zinnov as well as trade bodies such as NASSCOM. Examples of such reports are Gartner's and NASSCOM's reports referred to above.

The government of India has made Digital India one of its core missions and it is leveraging open, scalable and cost-efficient computing models to make this mission a reality. Given the cost-sensitive nature of the Indian market, the cost efficiencies offered by cloud computing will be core to making the Digital India mission successful.

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?

Currently, the government of India is considering a separate policy to create a separate legal framework for cloud computing. The Telecom Regulatory Authority of India released a consultation paper in 2016 on Cloud Computing in India and recommendations on cloud services in 2017 in furtherance of this.

The Ministry of Electronics and Information Technology (MEITY) addresses some aspects pertaining to cloud computing in its National Policy on Information Technology and the National Telecom Policy of 2012. One of the objectives of these policies is to develop an ecosystem to allow India to emerge as a global leader in the development and provision of cloud services. This focus is further enhanced in the National Digital Communications Policy 2018 released on 22 October 2018, which forms the overarching policy framework for all aspects of digital technologies in India over the next few years. The draft policy

envisages establishing India as a global hub for cloud computing, inter alia, through: (i) promoting the establishment of International Data Centres, Content Delivery Networks and independent interconnect exchanges in India; (ii) establishing a light-touch regulatory approach to cloud computing; and (iii) establishing captive fibre networks. Hence, it seems reasonable to expect a growing and beneficial policy focus on cloud computing in India over the next few years.

Incentives

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

Currently, there are no government schemes or policies that provide incentives or grants specifically to enterprises in the cloud computing sector. Fiscal incentives are extended to enterprises in certain categories such as:

- export-oriented enterprises set up inside special economic zones as notified by the government; and
- start-up ventures that are engaged in innovation and development of products, processes or services through use of intellectual property and technology, or that have a scalable business model with a high potential of employment generation or wealth creation. (A start-up is an entity incorporated or registered as a company or registered partnership or limited liability partnership less than seven years from the date of its incorporation or registration, that has a turnover less than 250 million rupees).

MEITY has, by way of the Public Procurement (Preference to make in India) Order 2017 (Order), stated that purchase preference (amounting to 50 per cent of total procurement) should be provided to local suppliers in all procurements to be undertaken by procurement entities in India as part of government of India's 'Make in India' policy with a view to enhance income and employment in India. Therefore, public sector procurement will favour domestic cloud computing providers.

Other than fiscal incentives, start-up ventures are allowed exemption from compliances under specific environmental and labour laws. Cloud computing providers that meet the aforesaid parameters will be eligible for these benefits.

LEGISLATION AND REGULATION

Recognition of concept

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

There is no legislation in India that specifically recognises cloud computing. However, cloud computing services would fall under the ambit of the following:

- 'Cloud services' have been specifically recognised under the Integrated Goods and Services Tax Act 2017 (the GST Act) under 'online information and database access or retrieval services' and therefore the services rendered by cloud services providers would be subject to goods and services tax.
- Section 43A of the Information Technology Act 2000 (the IT Act) read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the Privacy Rules) provide guidelines for the collection, use and protection of any sensitive personal data or information of natural persons by a body corporate that possesses, deals with or handles such data. The IT Act and the Privacy Rules together set out the regulatory framework for creation, collection, storage, processing and use of electronic data (including personal and sensitive personal information recorded in electronic form) in India. Cloud computing services that deal with personal or sensitive personal information need to comply with the requirements set out under the Privacy Rules relating to security, encryption, access to data subject, disclosure, international transfer and publication of policy statements. Cloud service providers in India may also be required to comply with the Information Technology (Intermediaries Guidelines) Rules 2011 (Intermediary Guidelines) prescribed under the IT Act.
- The government has a published a Personal Data Protection Bill 2018 (the Bill), which if notified will overhaul the existing privacy and data protection framework in India. The Bill is in many respects similar to the EU's General Data Protection Regulation and it, inter alia, enhances the stringency of obligations and corresponding penalties governing data protection from a customer perspective. The Bill has also set high standards for the processing of personal data within India and abroad and is expected to replace or amend the IT Act and the Privacy Rules in these respects. Data sovereignty has lately become one of the primary areas of concern of the Indian government, as national security could be compromised to threats in digital space. In pursuance of safeguarding data sovereignty, Indian legislature has proposed norms on data localisation in the Bill. Furthermore, the RBI, has mandated all payment system providers to store payment related data in systems in India. This data may include full end-to-end transaction details or information collected, carried or processed as part of the message or payment instruction. These norms have been introduced for the benefit of the local players in the cloud computing market. However, the draft e-commerce policy deviates from the relatively conservative position adopted in the Bill on data localisation insofar as it inter alia permits cross-border transfer of technology related data as long as it has no personal or community implications.

Governing legislation

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

As specified in question 8, there is no regulation in India that specifically prohibits, restricts or governs cloud computing. Question 8 describes the principal legislation that indirectly governs cloud computing services in India.

Other than the above, the use of cloud services by banks and insurance providers is separately regulated under sector-specific regulations.

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

Cloud computing services are primarily regulated (though indirectly) by the IT Act and Privacy Rules (see question 8).

In addition to the IT Act and Privacy Rules, the use of cloud computing in the banking and insurance sectors is subject to specific restrictions.

The RBI's guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks read along with the Report of Working Group of RBI on Electronic Banking set out specific requirements to be complied with by banks while engaging cloud service providers. These requirements, inter alia, relate to vendor selection, data security, form of agreement, business continuity and disaster recovery or management practices.

The Insurance Regulatory and Development Authority of India's Guidelines on Information and Cyber Security for Insurers require

insurers to comply with requirements, inter alia, in relation to data, application and network security, incident management, and information security audit while using services from a cloud service provider.

The government retains the authority to intercept any information transmitted through a computer system, network, database or software for the prevention of serious crimes or under grave circumstances affecting public order and national security.

See also the paragraph pertaining to the Bill (see question 8) and its proposed impact on obligations of entities with respect to privacy and data protection in India.

Breach of laws

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

The IT Act and Privacy Rules prescribe payment of damages on account of failure to or in case of negligence in implementing or maintaining reasonable security practices to protect any sensitive personal information. The non-compliant entity is required to pay damages to the aggrieved party to the extent of wrongful loss or damage suffered by the aggrieved party. Further, any person who has received any personal or sensitive personal information for performing any services, and discloses it with a mala fide intent is liable to a fine of up to 500,000 rupees or imprisonment of up to three years, or both.

The sector-specific regulations (see question 10) set out sanctions by regulators in case of non-compliance with them, which could range from fines to suspension or revocation of the licence to carry on business.

It is important to note that the Bill proposes to impose heavy monetary sanctions involving a percentage of total worldwide turnover, for non-compliance with the privacy and data protection measures laid down by it. There is good reason to believe that this position will prevail when the law comes into force.

Consumer protection measures

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

The IT Act provides for the following consumer protection measures:

- the IT Act (and therefore the penal consequences of the Act) covers offences committed outside of India if the offence involves a computer, computer system or computer network located in India. This would protect consumers within India who procure cloud computing services from service providers located outside India;
- the Privacy Rules protect consumers by casting obligations on cloud computing providers with regard to the collection and storage of personal information. These include broadly:
  - disclosures to be made to such users or consumers regarding the fact that the information is being collected or stored;
  - the purpose of collection;
  - the manner in which such information can be transferred; and
  - the minimum-security practices and procedures to be implemented by cloud service providers when processing personal information.

The Consumer Protection Act 2019 (which is yet to come into force) grants the right to the central government to make rules for measures to be taken to prevent unfair trade practices in e-commerce, direct selling and also to protect the interest and rights of consumers in this regard.

Indian regulators are increasingly focused on all aspects relating to data protection and data localisation. The RBI recently mandated that all providers of payment systems must ensure that all data relating to payment systems operated by them are only stored in systems within India. The new Bill also proposes to enhance consumer protection measures by introducing data localisation requirements wherein in respect of cross-border transactions, a data controller is required to maintain at least one copy of personal data on a server or a data centre in India. This in turn would, inter alia, have the effect of relative ease in enforcement of claims by customers under consumer protection laws.

Sector-specific legislation

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

See questions 8 and 10.

Insolvency laws

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

There is no specific law in India that determines what happens to any data of the customer once the cloud service provider becomes insolvent and this would ideally be governed by the contract between the service provider and the customer.

The Companies Act 2013, as amended by the Insolvency and Bankruptcy Code 2016, governs procedure to be followed when a company becomes insolvent. In the absence of any contractual understanding regarding the treatment of customer data in case of insolvency of the service provider, the liquidator of the company will decide how such data would be treated.

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.

The IT Act and Privacy Rules (see question 8) is currently the primary legislation governing data protection and privacy with respect to cloud computing in India. However, on 24 August 2017, a nine-judge bench of the Supreme Court of India conclusively held that the right to privacy is a fundamental right guaranteed to the citizens of India (subject to reasonable restrictions) and such right would also be exercisable against the state. See question 8 for more details on the proposed changes in the privacy and data protection framework in India that resulted from this decision of the Supreme Court.

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)?

The most common form of cloud computing contracts in India are international standard form contracts with fixed terms and are in most instances non-negotiable, with certain exceptions. However, if the cloud service provider is a small service provider the user may have more room to negotiate terms. The terms of the contract will also depend on the service delivery model (ie, whether it is IaaS, SaaS or PaaS).

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?

Under Indian laws, parties to a contract have the right to choose the governing law. However, in the event of a dispute, the courts will not only take into consideration the governing law as included in the contract but also its link with the contract. Usually, parties agree to the exclusive jurisdiction of the courts in the same country as the governing law.

Under section 44A of the Indian Code of Civil Procedure 1908, a decree of any superior court of a reciprocating territory that is so declared by the government, will be executed in India similar to any decree passed by a district court in India. All other judgments or decrees will face extensive re-adjudication in Indian courts.

Arbitration is a fairly commonly accepted method of dispute resolution. Parties should ideally also include an escalation clause for dispute resolution.

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?

Given the prevalence of international standard form contracts in the Indian market, the typical terms are similar to terms that are commonly used in large markets such as the US and the UK.

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?

Data security and confidentiality obligations are very important as users may upload confidential and proprietary information as well as personal data. The Privacy Rules prescribe that sensitive personal information should be stored in ISO 27001-compliant data centres. Clauses surrounding data privacy, confidentiality and data transfer, and preservation are largely similar to clauses found in international standard form contracts prevalent in the US and UK. Once the Bill becomes law, there will be significant changes on the data front.

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?

Clauses around liability, warranties and provision of service are solely dependent on the contractual arrangement reached between the parties. Most service providers will have standard service availability and service levels specified in the agreement that they would not be willing to negotiate. Similarly, most service providers would have standard business continuity and disaster recovery processes in place.

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?

Under a B2B public cloud computing contract, the service provider or its licensors will continue to hold all rights, title and interest in the cloud computing resources, while the user will continue to hold all rights, title and interest in the data it uploads as well as in any output that is generated through the use of such data.

Usually, a typical (and, in most instances, the only) indemnity that the service provider may be willing to provide is for indemnification for third-party intellectual property infringement claims and such indemnity is not capped.

Typical terms covering termination

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

Apart from termination rights set out in the agreement, a party has a statutory right to terminate in case of a breach by the other party. Other than that, a party whose consent to an agreement is obtained through coercion, fraud or misrepresentation can elect to terminate it. Most agreements may also contain a right for both parties to be able to terminate for convenience without incurring any liability.

In the instance the service provider is dependent on a third-party for essential services required to provide the cloud computing services, the services provider may retain the right to immediately terminate without incurring any liability if the service provider's relationship with the third-party is affected in any manner.

Post-expiry or on termination of the agreement, the agreement will usually provide for payment of any fees due and payable as well as refund of fees for services not rendered (though this may not be something larger cloud service providers may agree with). Provisions regarding return of user data are also included, with the service provider specifying the duration that they are willing to retain such data post which the data may be irretrievably deleted. The parties should also agree on the format in which the data would be returned. Most service providers will not agree on any further post-termination obligations. However, if the agreement is negotiable the user can ask for data retrieval, transfer or migration services.

Employment law considerations

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

There are no such labour or employment law considerations that would apply to a business customer.

TAXATION

Applicable tax rules

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

Providers of cloud computing services are subject to both direct and indirect taxes.

Direct taxes apply to the income of the cloud computing company and are collected on a combination of withholding at source and direct remittance by the cloud computing company.

As a consumer of goods and services, the company would mostly have a responsibility to bear the economic burden of tax specified under

the GST Act. The provider of goods and services, generally, has the responsibility of collection and remittance of the goods and services tax.

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.

Provision of cloud computing services from within India to a recipient also within India will attract goods and services tax (currently, at a composite rate of 18 per cent) under the GST Act. Where cloud computing services are exported and, therefore, consumed outside of India, the rate of applicable goods and services tax is zero (subject to meeting certain requirements).

The GST Act replaces the earlier service tax regime. As per the GST Act, cloud service providers are now able to claim credit on the input hardware used for providing services.

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 government recently launched a National Cloud Initiative – GI Cloud – to optimise the government's spending on internet and communications technology and to facilitate large-scale adoption of cloud computing and services within the governance mechanism. MEITY has provisionally accredited private cloud service providers for the development of cloud infrastructure. Currently, NIC Cloud (cloud.gov.in), a government website, offers service models such as PaaS, IaaS, SaaS and storage-as-a-service.

Further, given the pervasiveness of cloud computing today, a number of private and quasi-governmental organisations have formulated draft models for the development of cloud services in India. For example, the Cloud Computing Innovation Council published a white paper titled 'A Framework and Roadmap on Cloud Computing Innovation in India' that sets out a proposed roadmap for the development of cloud computing services in India through three phases:

- establishment of National Cloud Authority;
- setting up government clouds based on the certain interoperability standards emerged within India; and
- adoption of these interoperability standards by other Indian cloud companies on a large scale.

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?

See questions 8 and 10.

MC M MANI CHENGAPPA MATHUR

Samuel Mani
samuel@mcmlaw.in

Rosa Thomas
rosa.thomas@mcmlaw.in

Divyasri No. 26, SBI Colony
3rd Block Koramangala
Bangalore 560034
India
Tel: +91 80 4148 1999
www.mcmlaw.in

Japan

Atsushi Okada and Hideaki Kuwahara*

Mori Hamada & Matsumoto

MARKET OVERVIEW

Kinds of transaction

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

Public and private cloud models are both common in Japan. In the public cloud model, multiple users share a single cloud environment provided by a cloud provider, and in the private cloud model, a company builds its own cloud environment for its use or use by its group companies. While both are expanding their market sizes year on year, currently, private cloud models have a larger share. The preference for most Japanese companies currently seems to be the private cloud model, probably because of concerns about the security level of public cloud environments. A recent trend within the private cloud model is the increasing use of the 'community cloud', where a limited number of companies share a private cloud, which is more cost-effective than an ordinary private cloud, which requires a user to construct their own cloud environment. Various types of cloud computing services, including software-as-a-service, infrastructure-as-a-service and platform-as-a-service, are provided by many prominent cloud providers.

Active global providers

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

International cloud computing providers in Japan include Amazon.com, Microsoft, Google and IBM for both public and private cloud computing services.

Active local providers

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

Local cloud computing providers in Japan include NTT Communications Corporation, NTT DATA Corporation, KDDI Corporation, Softbank Group Corporation, Fujitsu Limited, NEC Corporation and Internet Initiative Japan Inc. These entities provide both public and private cloud computing services.

Market size

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

Cloud computing in Japan is fairly well established and has been constantly evolving. The market is currently valued at about ¥700 billion and is expected to increase up to about ¥1,200 billion by 2023. The majority of Japanese companies now use cloud services, it being especially popular among finance and insurance companies, and large-cap companies. Companies use cloud computing services for various purposes such as inter- and intra-office communication, preserving and sharing data electronically, operating company servers and portal sites.

Impact studies

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

The Ministry of Internal Affairs and Communications (MIAC) issues a white paper on telecommunications annually, which contains the results of surveys that MIAC conducts regarding the cloud computing market. Further, think tanks such as Nomura Research Institute publish statistics and analyses of the current and future cloud computing market. According to the IT Navigator 2018, published by Nomura Research Institute, users of traditional network services such as leased line have been decreasing in recent years and their market sizes shrinking, in contrast to the rapid expansion of the cloud computing market.

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 Japanese government established the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) within the Cabinet in January 2001. This organisation is tasked with promoting measures for an advanced information and telecommunications network society, expeditiously and intensively. Further, to encourage collaboration between the government, industry and academia in cloud computing services, the MIAC, the Ministry of Economy, Trade and Industry (METI) and the Ministry of Agriculture, Forestry and Fisheries, have established the Japan Cloud Consortium. This is a private sector organisation with more than 400 member corporations or organisations, and provides a forum for the members to share information on cloud computing services. MIAC in discussion with ASP-SaaS-Cloud Consortium, a non-governmental organisation, deals with matters regarding the provision and use of cloud computing services and guidelines regarding security issues. Moreover, MIAC regularly engages in discussions with foreign countries regarding security issues in 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?

Government authorities such as METI and the Tokyo Metropolitan Government grant subsidies to businesses aiming to introduce cloud computing services that use data centres with high energy efficiency, with a view to promoting energy conservation.

LEGISLATION AND REGULATION

Recognition of concept

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

Although there are numerous legal issues pertaining to cloud computing, as we discuss below in detail, current Japanese statutory laws do not define cloud computing as a specific area of service to which certain restrictions or regulations apply.

Governing legislation

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

There is no legislation or regulation that directly and specifically prohibits, restricts or otherwise governs cloud computing in or outside Japan.

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

Under the Telecommunications Business Act (TBA), if cloud computing services include (i) telecommunications between the cloud provider and the customer and (ii) mediating telecommunications between two or more customers, then the cloud provider has either to file a notification or (if the cloud provider falls within the categories stipulated in TBA) register as a telecommunications carrier with the MIAC.

Under the Foreign Exchange and Foreign Trade Act, when a person or entity preserves data regarding certain technologies in servers located in foreign countries, that person or entity must obtain prior permission from METI. However, the interpretational guidelines issued by METI have clarified that if a customer preserves information in an overseas server of the cloud provider for the customer's own use, then such permission is not necessary.

Breach of laws

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

A person who breaches the obligation described in the first paragraph of question 10 is liable to be punished by imprisonment with labour for no more than three years or a fine of no more than ¥2 million under the TBA.

Consumer protection measures

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

First, with respect to business-to-consumer (B2C) cloud service agreements, certain provisions that could be considered unfair to an individual customer who does not execute the agreement on business (defined as a 'consumer') would be nullified under the Consumer Contract Act. Such provisions include:

- totally exempting the cloud provider from liability to compensate the consumer for damages arising from default or tort by the cloud provider;
- partially exempting the cloud provider from liability to compensate the consumer for damages arising from default or tort by the cloud provider (limited to default or tort owing to the cloud provider's intentional act or gross negligence);
- setting an agreed amount of liquidated damages or establishing a fixed penalty in the event of cancellation, which amount or penalty would exceed the normal amount of damages that would be payable to the cloud provider as a result of the cancellation of a contract, when compared to other contracts of the same type; and
- limiting the consumer's right to terminate the cloud service agreement when the cloud provider is in default.

Second, the Act on General Rules for Application of Laws also includes a rule to protect consumers. Under this rule, if the governing law in a cloud service agreement is a law other than the law of the consumer's habitual residence, and the consumer has manifested his or her intention to the cloud provider that a specific mandatory provision from within the law of the consumer's habitual residence should be applied, such mandatory provision would apply to the matters stipulated by such mandatory provision with regard to the formation and effect of the cloud service agreement.

And third, under the Japanese Code of Civil Procedure:

- a consumer would be able to sue the cloud provider in a Japanese court if the consumer's residence is in Japan at the time the cloud service agreement is executed; and
- the cloud provider would not be able to sue the consumer in a foreign court that both parties have agreed has the jurisdiction unless:
  - the consumer's habitual residence was in the foreign country when the cloud service agreement was executed; or
  - the consumer sues the cloud provider in the foreign court or agrees to defend himself or herself against the cloud provider's claim in the foreign court.

Sector-specific legislation

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

When a medical institution uses a cloud computing service to handle its patients' sensitive information, such as diagnostic records, maintaining the security of the cloud environment that stores such information is of crucial importance. Therefore, the Ministry of Health, Labour and Welfare, METI and MIAC each issue several guidelines that require such medical institutions to select a cloud provider that has a reliable security code and system, execute an agreement that ensures the cloud provider's proper handling of the confidential information (including prohibiting the provider's unauthorised browsing or analysis of the information) and oblige the medical institution to regularly supervise the cloud provider.

Additionally, a financial institution that uses a cloud computing service for its customers' confidential information is required to follow certain laws and guidelines regarding the security of the cloud computing service to which it outsources the handling of such information.

For example, the relevant financial laws and regulations, such as the Banking Act and the Financial Instruments and Exchange Act, require that if a financial institution preserves customer information through cloud computing services, it must establish the necessary

systems for maintaining the security of such information and for supervising the cloud provider to which it has delegated the handling of such information.

Further, the Center for Financial Industry Information Systems authorised by the Cabinet Office issued a report in November 2014, recommending that financial institutions take the following measures to ensure the proper handling by the cloud provider of customer information:

- conducting due diligence when selecting a cloud provider and executing a service agreement with the cloud provider;
- requesting the cloud provider to disclose information regarding the operation of the service and security management system;
- ensuring the proper operation of the cloud computing service including encryption of the confidential information and maintenance of the storage devices;
- upon the termination of the cloud service agreement, deleting, or having the cloud provider delete, the data, and/or transfer it to another cloud provider; and
- supervising the cloud provider's handling of the confidential information (including through on-site inspections).

Insolvency laws

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

If a cloud provider is subject to a ruling for the commencement of bankruptcy proceedings, the cloud service agreement, which is typically categorised as a quasi-mandate (Jun-inin) contract, will automatically terminate pursuant to the Japanese Civil Code, unless the parties have stipulated otherwise in the agreement.

On the other hand, if a cloud provider is subject to a ruling for the commencement of rehabilitation proceedings, the cloud service agreement will not automatically terminate, although a customer may terminate the agreement if the cause of termination (such as the cloud provider's breach of the agreement) has already existed before the commencement of rehabilitation proceedings.

If the cloud service agreement does not automatically terminate or is not terminated by the customer, the trustee of the cloud provider as appointed under bankruptcy laws can decide whether the cloud provider should continue the agreement or terminate it under Japanese bankruptcy laws. If the agreement is terminated, the customer can request the trustee to return its data stored in the cloud provider's server, regardless of whether there is a specific provision in the cloud service agreement that enables the customer to do so. However, under the current laws in Japan, it is unclear whether the customer can request the trustee to destroy or delete the data from the cloud server completely.

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.

Unless the cloud service agreement prohibits a cloud provider from handling personal information provided by a customer (eg, where the personal information is stored in a data centre owned by the cloud provider but the personal information is not accessible to the cloud provider at all), the cloud provider is obliged to handle the personal information subject to the Act on the Protection of Personal Information (APPI). Such obligations include the following items:

- The cloud provider has an obligation to take necessary and appropriate measures to ensure the secure management of personal data (generally, personal information compiled in a database) (personal data).
- The cloud provider shall, in having its employees handle personal data, exercise necessary and appropriate supervision over the employees so as to ensure the security of the personal data.
- The cloud provider is prohibited from providing any personal data to a third party without the prior consent of the person who originally provided the personal data (data subject), unless exceptions to the consent requirement apply. An example of such exceptions is where the cloud provider delegates all or part of the handling of personal data to an outsourcing company. However, in that case, the cloud provider must exercise necessary and appropriate supervision over the outsourcing company to ensure the secure management of the personal data.

Under a provision of APPI regarding overseas data transfers, a cloud provider must obtain the prior consent of the data subject before it can transfer his or her personal data to a third party located in a foreign country.

However, the data subject's consent to overseas data transfers is not necessary if:

1 the foreign country is specified in the Personal Information Protection Commission Ordinance (the PPC Ordinance) as a country which has a data protection regime with a level of protection equivalent to that of Japan; or
2 the third-party recipient has a system of data protection that meets the standards prescribed by the PPC Ordinance.

For item (1), as of July 2018, the PPC Ordinance has not identified any such foreign country. However, the recent adequacy dialogue between Japan and the EU confirmed that the PPC intends to identify the EU as having an adequate data protection regime in 2018.

For item (2), under the PPC Ordinance, the standards of the data protection system that a third-party recipient outside Japan must meet are either of the following:

- there is assurance, by appropriate and reasonable means (typically by entering into a contract), that the recipient will treat the disclosed personal data in accordance with the principles of the requirements for handling personal data under the APPI; or
- the recipient is certified under an international arrangement, recognised by the PPC, regarding its system of handling personal information.

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)?

For cloud computing services that are rendered in Japan, most cloud providers usually provide these services on the same terms and conditions for all customers, especially in B2C contracts. The normal practice is to provide a standard cloud service agreement on their websites, which the users must accept in order to use the services.

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?

Standard cloud service agreements provided by cloud providers typically stipulate that the location of the cloud provider's head office is the governing law and the court that has jurisdiction over the head office is the court of first instance. However, conferring jurisdiction on a foreign court may sometimes be regarded as invalid under the Code of Civil Procedure, as described in question 12.

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?

Material terms commonly include a stipulation for fees to be calculated as a fixed-rate or measured-rate fee, to be paid by a customer to the bank account designated by the cloud provider.

It is also common to prohibit a customer from undertaking certain activities such as:

- infringing the cloud provider's or a third party's IP or other rights;
- altering or deleting data owned by the cloud provider or a third party that is stored in the cloud server;
- activities that may obstruct or endanger the cloud provider's systems or communication lines;
- pretending to be the cloud provider or a third party when using the cloud service;
- accessing the cloud provider's system or network without the authorisation of the cloud provider;
- transmitting illegal or otherwise harmful contents to the cloud server; or
- other activities that are illegal or otherwise immoral.

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?

It is common to require the cloud provider to implement necessary and reasonable security protection measures to secure the confidentiality of the customer's data. To implement the requirement, it is also common to allow the cloud provider to take certain measures including suspension of the service when the cloud provider recognises the risk of the customer's data being (or having been) divulged by, for example, a third party's unauthorised access or malfunction of the cloud provider's systems or communication lines.

However, there are provisions that exempt the cloud provider from all or part of liabilities arising from the security issues, described hereinafter. For example, some agreements stipulate that the cloud provider will not guarantee the thorough prevention of a third party's unauthorised access or use of the server, nor indemnify damages incurred by the customer resulting from known or unknown security weaknesses. Other agreements require the customer to make backups of the data that it stores in on the cloud server and to preserve the ID or password appropriately, and exempt the provider from any liability when such ID or passwords are used by a third party.

Some agreements allow the customer to select the country where the cloud server is located.

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?

In B2B cloud computing contracts, it is typical for the cloud provider and the customer to execute a service level agreement (SLA). Typical SLA terms include:

- the period during which the service is provided;
- the level of manpower of the support desk;
- the rate of operation and the management of data; and
- handling of system malfunction and level of security.
-

Many SLAs stipulate that if the cloud provider fails to meet the service level obligations, the customer may be exempted from paying part of the future service fees, or that the cloud provider will refund part of the service fee already paid.

Typical cloud service agreements include a provision that limits the cloud provider's liabilities. For example, many cloud service agreements set a cap on the damages to be paid by the cloud provider to the customer as a result of actions attributable to the cloud provider, and allow the customer to claim only direct and ordinary damages (and exclude indirect, special and consequential damages). Other typical cloud service agreements exempt the cloud provider from any liability when the cloud provider is not at fault (such as in case of a third party's unauthorised access, natural disaster, malfunction of systems or communication lines, or attack by a computer virus). It is also customary to stipulate that the cloud provider does not guarantee the commerciality, fitness for a specific purpose or non-existence of an infringement of third parties' rights.

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?

Many cloud service agreements provide that the ownership of the intellectual property in data or information stored on the cloud server belongs to the person or entity who stored the data or information on the server (ie, the customer). Some agreements allow the cloud provider to copy the data in limited situations, such as when the cloud provider has to repair the communication line or equipment.

Further, in order to prevent the customer from infringing third parties' rights and thereby causing the cloud provider to incur any liabilities towards the third parties, agreements also usually stipulate that the customer must not infringe a third party's rights when it uses the cloud services. If the customer breaches the obligation and stores content that infringes third-party rights on the cloud server, the cloud provider will be able to claim an exemption from liability for any third party claims as a result.

Typical terms covering termination

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

Many cloud service agreements allow the customer a simple termination option, whereby a customer may terminate the cloud service agreement without cause, just by giving prior notice. However, some agreements require the customer to use the service for a minimum period and if the customer terminates the agreement before the completion of such period, the customer has to pay a certain amount of money to the cloud provider.

Cloud service agreements also usually allow the cloud provider to terminate the agreement if the customer is in breach of its obligation under the agreement or the customer is adjudged insolvent or bankrupt, or is liquidated or the like.

In light of the security management of the data stored on the cloud server, it is customary to require the customer to download the data before the cloud service agreement is terminated or expired at the customer's own responsibility, and limit or deny access to the data after termination or expiry. The cloud provider, on the other hand, is required to delete all of the customer's data stored on the server to ensure the confidentiality of the data.

Employment law considerations

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

There are no Japanese labour or employment laws currently regulating cloud computing.

TAXATION

Applicable tax rules

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

If a foreign cloud provider does its business through a 'permanent establishment' (as defined in the OECD Model Tax Convention) located in Japan, which is likely to include the cloud server, then such a cloud provider will be subject to Japanese business income tax.

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.

Providing cloud computing services through telecommunication lines (typically, the internet), will be regarded as a 'provision of service using telecommunication'.

A provision of service using telecommunication will be subject to Japanese Consumption Tax if it is regarded as a 'domestic transaction'. If the service is provided to the customer whose residence is in Japan, then this will be regarded as a domestic transaction regardless of whether the cloud computing service is provided from within or outside Japan. In that case, Japanese Consumption Tax will be imposed on the customer.

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.

There are no notable cases, or commercial, private, administrative or regulatory determinations within the past three years in Japan that have directly involved cloud computing as a business model.

MORI HAMADA & MATSUMOTO

Atsushi Okada
atsushi.okada@mhmjapan.com

Hideaki Kuwahara
hideaki.kuwahara@mhmjapan.com

16th Floor, Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
Tokyo 100-8222
Japan
Tel: +81 3 5220 1821
Fax: +81 3 5220 1721
www.mhmjapan.com

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?

No update at this time.

The information in this chapter is correct as at October 2018.

Korea

Young-Hee Jo, Seungmin Jasmine Jung and Youngju Kim
LAB Partners

MARKET OVERVIEW

Kinds of transaction

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

A comprehensive variety of cloud computing services is being provided and being adopted by companies in Korea. Public, hybrid and private cloud models are all provided by cloud service providers. Cloud service users use cloud computing services in the form of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) or for mere storage, based on the particular user's needs. Cloud computing is in the process of being adopted in various sectors such as healthcare, finance and information communications technology. In particular, cloud computing has been widely adopted in the online gaming industry.

Active global providers

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

In general, most large global cloud service providers are active in Korea. Notably, Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud, Oracle Cloud, HP Cloud, Akamai and Rackspace have a presence in Korea.

Active local providers

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

There are numerous cloud computing service providers in Korea. The largest domestic cloud service providers are established companies in the information communication technology network providers, such as KT (KT Cloud) and SK (Cloud Z), and internal portal companies, such as Naver (NAVER Cloud) and Kakao.

Market size

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

Cloud computing is becoming more and more widely adopted in Korea, with legislation being adopted by each industry to relax the legacy restrictions that made it difficult to adopt cloud computing.

According to the Worldwide Public Cloud Services Market Forecast (2019) published by Gartner in April 2019, the amount of spending by end-users of public cloud services in Korea is estimated as follows:

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	174,207	196,530	220,103	244,684	271,235
Cloud Application Infrastructure Services (PaaS)	215,457	258,237	302,048	347,941	392,554
Cloud Application Services (SaaS)	778,711	962,156	1,167,356	1,366,834	1,574,564
Cloud Management and Security Services	195,045	228,866	263,468	300,665	337,992
Cloud System Infrastructure Services (IaaS)	577,251	696,982	828,838	979,971	1,147,494
Total	1,940,671	2,342,771	2,781,813	3,240,095	3,723,839

(Unit: one million won)

Impact studies

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

Data and studies on the impact of cloud computing are publicly available. For example, the Korea Association of Cloud Industry (KACI) periodically posts studies and data on its website and the government provides a dedicated cloud portal (K-ICT Cloud Innovation Center, www.cloud.or.kr). Based on these studies and data, cloud computing is likely to grow at a rapid pace in the Korean market and will affect traditional IT vendors and IT outsourcing.

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?

Yes. To promote and develop cloud computing services, Korea has adopted the Act on the Development of Cloud Computing and Protection of its Users (the Cloud Computing Act) to develop the cloud computing industry in Korea and to promote Korean cloud computing services to foreign customers.

Under the Cloud Computing Act, the government can conduct the following activities to promote international cooperation on cloud computing and overseas expansion of cloud computing technology and services:

- international exchange of cloud computing-related information, technology and personnel;

- overseas marketing and promoting activities such as cloud computing exhibits;
- joint research and development of cloud computing with other nations;
- information collection, analysis and provision regarding information related to the overseas expansion of cloud computing;
- mutual cooperation with other nations to ensure the effectiveness of international cooperation in relation to cloud computing; and
- other activities to promote international cooperation and overseas expansion of cloud computing.

Incentives

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

In order to develop and promote the use of cloud computing technology and services, the government and municipalities can adopt measures such as tax incentives. Also, the government can provide support to small and medium-sized businesses related to cloud computing such as the following:

- provide information and advice related to cloud computing business;
- subsidise funds and provide technology assistance for the purpose of user protection;
- training of cloud computing professionals; and
- other activities necessary with regard to fostering small and medium-sized businesses related to cloud computing.

Furthermore, the government and municipalities can provide administrative, fiscal and technical support to parties that are establishing collective information communication facilities using cloud computing technology.

LEGISLATION AND REGULATION

Recognition of concept

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

The Cloud Computing Act defines cloud computing, cloud computing technology and cloud computing service as follows:

Cloud computing

An information processing system that enables elastic use of integrated and shared resources for information and communications (such as devices for information and communications, information and communications systems, and software) through information and communications networks, to fit the users' requirements or demands.

Cloud computing technology

Technology required for setting up and using the cloud including the following:

- virtualisation technology: technology for virtually combining or dividing resources for information and communications including integrated or shared information and communications devices, information and communications facilities, and software;
- distributed processing technology: technology that processes a large volume of information by dispersing it into multiple information and communications resources; and
- others: technology that utilises information and communications resources in setting up and using cloud computing systems, including technologies that automate the placement, management and so on of information and communications resources.

Cloud computing services

Commercial services for providing resources for information and communications by utilising cloud computing including the following:

- service of providing servers, storage, networks, among others;
- service of providing software, including applications;
- service of providing an environment for developing, distributing, operating, managing, and suchlike, software, including applications; and
- other services combining at least two of the above services.

Governing legislation

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

The purpose of the Cloud Computing Act is to promote and develop cloud computing rather than to regulate cloud computing. Under the Cloud Computing Act, an agreement between the cloud computing service provider and the cloud service user will be deemed to satisfy the requirements for IT facilities, devices and systems that are necessary to obtain permits, approvals, registration or designations pursuant to other laws. However, the Cloud Computing Act does not contain explicit prohibitions. Rather, detailed measures that directly or indirectly restrict to cloud computing are contained in industry specific laws and the privacy laws of Korea. In other words, Korea adopts a negative regulatory approach, where cloud computing is generally permitted unless explicitly restricted by a specific statute.

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

For personal information protection in the cloud, the Personal Information Protection Act (the PIPA) and the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (the Network Act) apply. Accordingly, the collection, use, provision, delegation, destruction, storage of personal information being processed by cloud computing is subject to the PIPA and the Network Act. Both the PIPA and the Network Act contain stringent provisions to ensure the protection of data subjects with corresponding heavy penalties. Under the PIPA, a cloud computing service provider is considered a delegatee who has been delegated with personal information processing and is treated as a data processor.

With regard to data security, the Ministry of Science and ICT has promulgated 'Standards for Information Protection by Cloud Computing Providers' (Cloud Computing Standards). The Cloud Computing Standards do not have the effect of binding law but compliance therewith is, nonetheless, recommended.

Breach of laws

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

A cloud computing service provider could become subject to criminal penalties in the event the cloud computing service user's data is provided to a third party by the cloud computing service provider. As noted above, the Cloud Computing Standards do not have the force of law and therefore, in theory, the quality, performance and data protection levels stated therein are not mandatory. The failure to notify the occurrence of any infiltration incidents to the relevant authorities or to the users or return or destroy information will be subject to a fine. Furthermore, if the cloud service provider breaches any provisions of

the PIPA or the Network Act, the cloud service provider could be subject to a fine, corrective measure or criminal penalty based on the relevant statutory provisions.

Consumer protection measures

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

Pursuant to the Cloud Computing Act, the Ministry of Science and ICT, in consultation with the Fair Trade Commission, has published a model cloud computing agreement for business-to-business (B2B) and business-to-consumer (B2C), respectively. The purpose of this model agreement is to protect the rights of the users and to establish fair trade. The Ministry of Science and ICT can issue a recommendation to use this model agreement to cloud computing providers.

The model agreement includes the following protective measures:

- the PIPA and the Network Act will apply to personal information thereby reinforcing the protection of personal information;
- any incident of leakage of user information must be notified to the user and the Ministry of Science and ICT to enable prompt remedial measures with respect to such incident;
- to enhance the user's right to know, in the event the user's data is stored overseas, the user can demand disclosure of the country where data is stored and the fact that cloud computing is being used, with respect to which recommendation measures for disclosure can be issued; and
- to prevent the misuse of user data, any provision of user data to third parties without consent or use of user data beyond the agreed purpose shall be subject to criminal penalties.

Sector-specific legislation

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

Public sector

The Cloud Computing Act states the obligation of governmental agencies to use efforts to adopt cloud computing and recommends that governmental agencies use the cloud computing systems developed by the private sector rather than developing its own cloud computing system. To support the adoption of cloud computing in the public sector, a joint policy commission consisting of the Ministry of the Interior and Safety, the Ministry of Science and ICT, the Ministry of Economy and Finance, the Public Procurement Service and the National Intelligence Service has been set up. A security review by the National Intelligence Service is required for governmental agencies to adopt a certain cloud computing system.

Finance sector

The amendments to the Electronic Finance Supervisory Regulations announced by the Financial Services Commission became effective on 1 January 2019. These amendments allow personal credit information to be processed on the cloud while strengthening the security level and management supervisory systems of cloud computing used in the financial sector. The major amendments are as follows:

- The most important amendment is the expanded scope of cloud use that is permitted. In the past, financial institutions and electronic financial companies could only use the cloud to process non-critical information in the cloud. Now, under the amendments to the Electronic Finance Supervisory Regulations, the cloud can be used for personal credit information and personal identification information as well (article 14-2, sections 1 and 8).
- The amendments provide for a new finance-sector-specific standard for the use and provision of cloud services such as security measures applicable to the finance sector (article 14-2, section 1, Annex 2-2), which did not exist previously.
- The amendments impose a new obligation to financial institutions and electronic financial companies to assess the security of the data processing systems in the cloud and to conduct a review and decision process by their internal data protection committee (article 14-2, sections 1 and 2).
- The amendments reinforce the supervisory role of the regulatory authorities by requiring financial institutions and electronic financial companies to report the use of cloud services for personal credit information and personal identification information, for matters that materially impact the security and credibility of electronic financial transactions and for other critical events (article 14-2, sections 3 and 6).
- To ensure regulatory enforcement and consumer protection, only cloud computing providers whose data processing systems are in Korea can be used for processing personal information and personal identification information (article 14-2, section 8).

Healthcare sector

The amendment to the Standards on Facilities and Devices for Administration and Retention of Electronic Medical Records in 2016 has paved the way for the adoption of cloud computing in the healthcare sector. The amendment revises the requirement to store electronic medical records inside hospitals and allows the administration and storage of medical records with external companies or at remote locations that meet certain qualifications. However, electronic medical records cannot be stored outside of Korea.

Insolvency laws

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

There are no insolvency laws that only apply to cloud computing service providers. However, the Cloud Computing Act contains a provision that applies when the cloud computing provider suspends its service due to reasons such as sudden insolvency. Under this provision, the cloud computing service provider and the user can agree to temporarily store the user's data with a third party. Also, if a cloud computing service provider intends to terminate its business, it must notify the user of such termination and return or destroy all data to the user prior to the date of termination of business. If, for any reason, it becomes impossible to return the information (for example, the user fails to accept, or refuses, the return of such information), the cloud computing service provider must destroy the information.

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.

The PIPA and the Network Act apply to cloud computing service providers in connection with data privacy. In principle, the privacy laws of Korea are structured to require the prior consent of the data subject for the collection, use and provision of personal information. Within personal information, sensitive information and personal identification information is subject to more stringent regulations. Under the PIPA and the Network Act, overseas provision of personal information to third parties requires the consent of the data subject. The overseas delegation of personal information processing to third parties does not require the consent of the data subject under the PIPA, whereas consent is required under the Network Act.

A personal information processor must take technical, organisational and physical measures stated in the privacy laws to ensure against the loss, theft or leakage of personal information. Upon leakage of personal information, the personal information processor must notify the data subject and the relevant authorities without delay. Any violation of the privacy laws may be subject to administrative sanctions or criminal penalties. In particular, any loss, theft, leakage, alteration or damage to personal information due to the lack of the security measures under the PIPA or the Network Act will be subject to a criminal penalty of not more than two years' imprisonment or a monetary penalty of not more than 20 million Korean won (article 73 of PIPA and article 73 of the Network Act).

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)?

In practice, cloud computing contracts usually adopted in Korea are similar to those globally used by cloud computing service providers. Many cloud computing service providers adopt modular agreements composed of several different components such as:

- a master agreement between the customer and cloud servicer provider;
- service level agreements and terms for each service;
- the cloud service provider's acceptable use policies; and
- end-user licence agreement.

Often these agreements are presented as clickwrap agreements with non-negotiable terms. Accordingly, to protect the rights of the cloud service users, the Ministry of Science and ICT has published a model agreement that is analysed in questions 17 to 22.

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?

Article 24 of the Cloud Computing Act states that the Ministry of Science and ICT, in consultation with the Fair Trade Commission, may establish a model agreement for cloud computing to protect the rights of cloud computing users and establish fair trade practices. In December 2016, the Ministry of Science and ICT published two versions of the Model Cloud Agreement for Protection of Cloud Service Users and Establishment of Fair Trade Practices, one for B2B and one for B2C.

Under the Model Cloud Agreement for Protection of Cloud Service Users and Establishment of Fair Trade Practices for B2B (B2B Model Agreement), Korean law is the governing law and any disputes arising out of the agreement are subject to the jurisdiction of the Korean court.

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?

Under the B2B Model Agreement, the cloud service provider must provide cloud computing services in accordance with the B2B Model Agreement, and the specific service levels will be subject to the service level agreements. Any modifications to the service levels should be mutually discussed, provided that any modifications that are material or are contrary to the interests of the cloud computing user are subject to the user's consent.

The B2B Model Agreement divides service fees into basic fees and ancillary fees. The details of the service fees (type, price, method of pricing, discounts, etc) must be listed in an attachment to the B2B Model Agreement or on the service website. In principle, the service fees are on a monthly basis and prorated on a daily basis upon termination. Any discount or waiver of fees can be determined based on mutual discussion. In the event of temporary suspension or disruption of services, the user will be entitled to request discount of the service fees or seek damages arising from such suspension or disruption.

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?

Under the B2B Model Agreement, the cloud computing provider must:

- adopt the Cloud Computing Standards;
- provide adequate security measures; and
- ensure protection against leakage of personal information and third-party infiltration.

Further, the cloud computing provider cannot provide the user's information to a third party without the user's consent or use the user's data beyond the agreed purpose. The user is responsible for controlling its ID and password and bears responsibility for any theft or inappropriate use due to the user's failure to exercise due care.

Data protection measures not stated in the B2B Model Agreement will be subject to the privacy laws such as the PIPA, Network Act or industry-specific laws based on the user's business.

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?

In general, under the B2B Model Agreement, the cloud computing service provider is liable for damages incurred by the user owing to intentional or negligent service disruptions or for failure to meet the level of quality or performance of the services under the relevant service level agreement.

However, absent any intentional misconduct or negligence, the cloud computing service provider will not be liable for the user's damages because of:

- inevitable service interruption due to system upgrades, prevention of infiltration such as hacking or network failure, force majeure events that have been notified to the user pursuant to the B2B Model Agreement;
- service suspension due to force majeure events beyond the control of existing technical capability;
- service suspension, disruption or termination of the B2B Model Agreement owing to the user's intentional misconduct or negligence;
- the network service provider's discontinuation or disruption of network services;
- ancillary issues arising from the user's computer environment or network environment; and
- the user's computer error or erroneous identification information or incorrect email address.

Further, the cloud computing provider is not liable for the credibility or accuracy of the information or material transmitted using the services or posted on the service website absent any intentional misconduct or negligence.

Additionally, the cloud service provider will not be liable in disputes regarding cloud computing services between users or between a user and a third party if all of the following conditions are met:

- the cloud computing service provider has not violated the Cloud Computing Act;
- the cloud computing service provider has proved that there is no intentional misconduct or negligence on its part;
- the cloud computing service provider does not have the authority or capacity to control the acts of the user that is infringing on the rights of other users or third parties;
- even if the cloud computing service provider does have the authority or capacity to control the user against the infringement of the rights of other users or third parties, the cloud computing service provider does not financially benefit from such infringement; and
- the cloud computing service provider immediately suspends the infringement once it becomes aware of the fact or circumstances that a user or third party is infringing on the user's rights.

On the other hand, if the user has caused damages to the cloud computing service provider, it will be liable for the damages incurred by the cloud computing service provider.

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?

Under the B2B Model Agreement, the user must not violate the Copyright Act and related laws or moral customs and social order. Further, absent any intentional misconduct or negligence, the cloud computing service provider will not be liable for any infringement on IPR between users or between a user and a third party. Other matters concerning IPR ownership are not specifically mentioned in the B2B Model Agreement and would, therefore, be subject to the intellectual property laws of Korea.

Typical terms covering termination

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

Under the B2B Model Agreement, both the cloud computing service provider and the user can rescind or terminate the B2B Model Agreement. The termination rights of the cloud computing service provider and user are as follows.

User

- Cloud computing service provider is unable to or there is a materially adverse effect on its ability to perform its obligations;
- the cloud computing service provider fails to provide services as contracted; and
- a material event has occurred that makes is impossible to maintain the contractual relationship.

Cloud computing service provider

- The user violates its obligations such as payment default or assigns its rights to a third party without the consent of the cloud computing service provider;
- a user whose use has been restricted under the B2B Model Agreement fails to cure the cause for such restriction for a substantial period of time; and
- the cloud computing service provider terminates its cloud computing business.

The cloud computing service provider must return the data to the user upon the rescission, termination of the B2B Model Agreement or upon expiry of the service term. If the return of data is practically impossible, the cloud computing service provider must destroy the user data in an irreversible manner. The cloud computing service provider must also cooperate in transferring the user's data to a different cloud computing service.

Employment law considerations

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

There are no labour or employment laws specific to the cloud computing industry.

TAXATION

Applicable tax rules

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

In general, to establish a corporation in Korea, a capital registration tax of 0.48 per cent of the initial capital applies. After establishment of the corporation, VAT, corporate income tax and local income tax will apply and other taxes such as withholding tax and municipal tax may also apply. It is notable that VAT applies to cloud computing services provided by Korean companies. Corporate income tax will be imposed at the following tax rates:

Tax basis (Korean won)	Tax rate*
200 million or less	10 per cent
200 million up to 20 billion	20 million + (20 per cent of the excess over 200 million)
20 billion up to 300 billion	3.98 billion + (22 per cent of the excess over 20 billion)
More than 300 billion	65.58 billion + (25 per cent of the excess over 300 billion)

* Local income tax equivalent to 10 per cent of the corporate income tax calculated based on the above will apply.

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.

The Value-Added Tax Act has been amended and become effective as of 1 July 2019 to include cloud computing services as one of the taxable electronic services provided by foreign corporations (article 53, section 1, paragraph 3). This amendment was made to ensure tax equality between Korean corporations and foreign corporations. As a result of this amendment, foreign cloud service providers are obligated to charge a 10 per cent VAT.

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.

As of yet, there are no such cases or determinations relating to cloud computing as a business model.

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?

Important changes were made with respect to cloud computing in 2019, most notably the expanded scope of cloud use permitted in the finance sector and the imposition of VAT to cloud services provided by foreign corporations. Nonetheless, there are still regulatory hurdles that make full-scale cloud adoption difficult. One of the main barriers to the proliferation of cloud adoption are the strict data privacy laws of Korea. According to the 2018 cloud industry survey conducted by the Ministry of Science and ICT and the National IT Industry Promotion Agency, 47.8 per cent of cloud service providers cited 'security' as an obstacle to the development of the cloud computing industry. Under the current privacy laws such as the Personal Information Protection Act and the Network Act, the adoption of cloud computing is deemed delegation of data processing, and, therefore, requires compliance with the strict requirements for delegation. Such strict requirements are often not compatible with the nature of cloud computing, thereby making companies hesitant to adopt cloud computing. Accordingly, there are discussions as to whether the Cloud Computing Act should prevail over privacy laws to enable widespread adoption of cloud computing.

LAB PARTNERS

Young-Hee Jo
yhjo@labpartners.co.kr

Seungmin Jasmine Jung
smjung@labpartners.co.kr

Youngju Kim
yjkim@labpartners.co.kr

8th Floor, VPLEX
501 Teheran-ro, Gangnam-gu
Seoul 06168
Korea
Tel: +82 2 6956 0250
Fax: +82 2 6956 0280
http://labpartners.co.kr

Sweden

Peter Nordbeck and Dahae Roland
Advokatfirman Delphi

MARKET OVERVIEW

Kinds of transaction

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

The demand for and use of cloud-based services in Sweden is rapidly growing. There is also an increased focus on information security due to additional requirements in this respect when processing critical or sensitive information. The services and cloud infrastructure vary depending on the users' requirements and needs. There are three internationally established types of cloud services that describe three different function areas: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS). All three are used on the Swedish cloud service market to various extents.

In a recent study carried out by the Swedish Pension Agency determining the most used services among public authorities in Sweden, the Agency concluded that IaaS was used by 30 per cent, PaaS by 23 per cent and SaaS by 78 per cent. This may lead to a conclusion that SaaS is the most common cloud service used by Swedish authorities (source: Pensionsmyndigheten – Molntjänster i staten – En ny generation av outsourcing).

Reports from 2016 and 2018 that examined the private sector's use of cloud services present similar conclusions. Out of the top 250 Swedish public cloud computing providers, SaaS constitutes 74 per cent of the segment, while IaaS represents 26 per cent. Out of the SaaS providers, 67 per cent use IaaS partners, out of which 36 per cent of the infrastructure providers are located in Sweden. The remaining SaaS providers have their own infrastructure. Recently, Sweden has also seen an increase in the number of SaaS providers owing to an uptake in the number of e-commerce services, fintech development and general digitalisation (source: METISfiles – Cloudscape Sweden V1.1, September 2016 and METISfiles – Cloudscape Sweden V1.2, September 2018).

When looking at the different models for providing cloud services in Sweden, the NIST and ISO standard describe four ways of service deployment: public clouds, partner clouds, hybrid clouds and private clouds. Hybrid clouds are quite common in both the public and private sector, and reports are stating that the use will probably increase in the future. Among public authorities, partner clouds are often used to ensure that all security requirements are met, which has been a concern in the use of public clouds (source: *Pensionsmyndigheten – Molntjänster i staten – en ny generation av outsourcing*).

Recently, Sweden has had numerous notable cloud transactions and has been described as a leading country when it comes to innovation and risk capital investment. Just a few years ago, Amazon moved part of its cloud service, Amazon Web Service (AWS), to Sweden and representatives of AWS have stated that AWS is planning to increase its presence in the Nordic countries without mentioning any cities targeted for the expansion.

Active global providers

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

Sweden is an attractive market for cloud providers and many of the international providers are active within Sweden. Many Swedish SaaS providers prefer to use a Swedish IaaS partner; however, the largest hosting partner within Sweden is Amazon (US) that represents 43 per cent of the segment, followed by Microsoft, DGC and IP-Only. Other international cloud providers active in Sweden are giants such as Google, Dropbox, LinkedIn, Facebook and iCloud; however, this is not a conclusive list (source: METISfiles – Cloudscape Sweden V1.1, September 2016 and METISfiles - Cloudscape Sweden V1.2, September 2018).

Active local providers

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

There are numerous Swedish cloud service providers. Important local IaaS providers are, inter alia, Atea, Bahnhof, Evry, Knowit and Tieto. These providers are common hosting partners to SaaS providers. Among the top Swedish SaaS providers are iZettle and Klarna (payment), Truecaller and Tele2 (communications), and Ericsson. There are fewer Swedish PaaS providers. However, local PaaS providers that can be mentioned are Accedo, Bariumlive and Cloudnet (source: METISfiles – Cloudscape Sweden V1.1, September 2016 and METISfiles - Cloudscape Sweden V1.2, September 2018).

Market size

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

The cloud adaption in Sweden is among the largest in Europe – in 2018, 57 per cent of Swedish enterprises used cloud computing services. Only Finland had a higher share of enterprises using cloud computing services in the European Union (source: Eurostat – Cloud computing: statistics on the use by enterprises, December 2018). The total cloud computing market in Sweden was valued to 16 billion krona in 2016 and the annual growth is currently estimated to be around 30 per cent (source: *Framtidens Karriär – Kostnadsjakt driver molntillväxt, 2017-02-07*).

Impact studies

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

There are some reports published regarding cloud computing in Sweden. A notable report on cloud computing's impact on state agencies was published by the Swedish Pensions Agency in January 2016.

The Swedish Pensions Agency concluded in its report that factors such as innovation, cost-efficiency, flexibility and accessibility are strongly benefited by the use of cloud services. Furthermore, the report concludes that cloud services could have a positive effect on the cooperation between authorities and simplify the access to governmental data and services (source: *Molntjänster i staten – En ny generation av outsourcing, Pensionsmyndigheten,* January 2016).

The Swedish Civil Contingencies Agency and the Swedish Data Protection Authority (DPA) have published guidelines and policies for public authorities regarding, inter alia, information security requirements in the public procurement process for cloud services as well as privacy concerns that must be considered. The Swedish Civil Contingencies Agency has also published a study that maps the use of cloud services by public authorities and the risks associated with their use (source: *MSB - Studie, Säkerhet vid molnlösningar*).

In addition, the Swedish government has taken further steps to ensure continued digital growth. In 2016, it presented five strategic cooperation programme that will help meet several of the social challenges facing Sweden. To stimulate digitalisation of Swedish industry, the Swedish government is requesting extensive cooperation between different actors (source: *Regeringen – Strategiska samverkansprogram en kraftsamling för nya sätt att möta samhällsutmaningar*).

The research company METISfiles has published its report Cloudscape v. 1.2 2018: An Overview of the Swedish and Danish Cloud Market in English that examines the cloud market in these countries.

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?

Sweden is currently attracting foreign risk capital investors due to the fast digitalisation and innovation. Numerous governmental initiatives have been launched to ensure that Sweden continues to develop in the digital arena and to live up to future requirements regarding privacy, IT and security. As one step in this process, the Swedish government requested the Swedish Pension Agency to analyse and evaluate the potential for using cloud services within the public sector and by the state in a way that contributes to a simpler, more transparent and efficient management. Other steps consist of a strong focus on general digitalisation both within the administration and the private sector.

Incentives

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

Various grants are available for small to medium-sized companies for projects involving innovation and digitalisation and are awarded by the Swedish government, public agencies and other organisations. Support to large companies also occurs, one significant example being the regional investment grant of around 100 million kronor awarded by the Swedish Agency for Economic and Regional Growth when Facebook established server halls in Luleå in the north of Sweden in 2011. Grants also exist for the expansion of the Swedish IT infrastructure.

LEGISLATION AND REGULATION

Recognition of concept

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

There is no specific recognition of cloud services in Swedish legislation.

Governing legislation

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

As a general rule, Sweden lacks direct and specific regulation regarding cloud computing as such. Swedish legislations and regulations are in general technology neutral, which implicates that Swedish legislations lacks that sort of specific targeting. However, the legal concerns are regulated indirectly in several legislations and regulations. The most relevant regulations are MSBFS 2016:1 and MSBFS 2016:2 that regulate the public authorities' internal information security policies and work, as well as the requirement to report IT incidents to the Swedish Civil Contingencies Agency. Cloud services are regulated by explicit requirements for internal policies and routines regarding incident management, the requirement that organisations must be able to handle threats and risks through models and routines for incident and continuity management.

Sweden has implemented the NIS Directive (EU) 2016/1148 through the Act on Information security for vital societal functions and digital services (SFS 2018:1174), thereby extending the requirements on security and to report IT incidents to cloud service providers.

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

Regarding indirect regulations and legislation, there are several to take into account. When using cloud services to store data from telecoms or e-commerce business, it is important to observe the Electronic Communications Act (SFS 2003:389), which aims to provide individuals and authorities with secure and effective electronic communications, and the Electronic Commerce Act (SFS 2002:562), which states an obligation to provide certain information to customers.

However, the main legislation to take into account regarding cloud services are the provisions on privacy and information security. On 25 May 2018, the General Data Protection Regulation (GDPR) entered into force in Sweden and provides significantly stricter standards, for example, on impact assessments and information security.

Information security is regulated throughout different provisions, such as regulations from the Swedish Civil Contingencies Agency, the GDPR and sector-specific regulations, such as within the healthcare sector. Swedish public authorities are subject to the principle of public access to public documents, which means that all documents submitted to or drawn up by the authority are, in principle, public documents and must be made available for anyone to read. Exemptions from this rule are documents that are subject to statutory secrecy under the Public Access to Information and Secrecy Act (SFS 2009:400) (the Secrecy Act), which means that they may not be disclosed to any third party. In cases where such classified information will be processed in the cloud, additional restrictions regarding the data apply and must, inter alia, be taken into consideration when assessing the risks and which security measures must be implemented.

In addition, if information subject to secrecy under the Secrecy Act may be available to the provider as a result of an agreement between

the parties, it must be evaluated whether the data becomes 'disclosed' within the meaning of the Secrecy Act. Thus, one opinion is that the Secrecy Act generally prevents authorities from using cloud services. Another opinion is, however, that it is possible for authorities to use cloud services if the relevant authority has made a thorough assessment of the risks based on the character of the information, but further clarification on how these rules are to be interpreted is needed.

Furthermore, public authorities must also comply with numerous other pieces of legislation such as the Archives Act (SFS 1990:782), the Administrate Procedure Act (SFS 1971:291), the Public Procurement Act (SFS 2016:1145) and the Security Protection Act (SFS 1996:627). Also, many public authorities and agencies have sector-specific provisions regarding data processing and information security requirements such as the Patient Data Act (SFS 2008:355).

Breach of laws

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

The failure to report an IT incident under the Act on Information security for vital societal functions and digital services is subject to administrative fines. Further, the rules indirectly regulating cloud computing in Sweden are connected to several sanctions and consequences for breaches thereof. The sanctions for lack of compliance with the GDPR include prohibitory injunctions, payment of damages as well as administrative fines. Lack of compliance with the Electronic Communications Act (SFS 2003:389) and the Electronic Commerce Act (SFS 2002:562) may also cause sanctions, such as prohibitions and orders combined with penalties as well as damages and criminal proceedings. Breaches of the Secrecy Act (SFS 2009:400) may lead to disciplinary or criminal proceedings. There are also various sanctions of similar character for the sector-specific regulation as well as supervision from relevant public agencies.

Consumer protection measures

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

There is no cloud service-specific regulation protecting the rights of consumers in Swedish law, but the Swedish consumer protection legislation includes legislation with focus on e-commerce and digital transactions including Distance and Off-Premises Contracts Act (SFS 2005:59), Consumer Contracts Act (SFS 1994:1512) and the Electronic Commerce Act (SFS 2002:562). The standard Swedish consumer protection for buying goods and services, the Consumer Sales Act (SFS 1990:932) and the Consumer Services Act (SFS 1985:716), is not directly applicable on purchases of digital content, but is still considered to have an impact when courts are evaluating consumer contracts. The consumer protection legislation, inter alia, ensures the consumer rights in regard to quality and performance from the commercial actor, includes the right to withdraw from distance and off-premises contracts within 14 days, bestows a responsibility for commercial actors to provide consumers with information, and provides that courts can prohibit contract terms that are unfair towards consumers from further use and may interpret vague contract terms in favour of consumers. The Swedish consumer protection for digital services is also continuously affected by the EU digital single market reform, and now includes the right to settle disputes online through the Alternative Dispute Resolution For Consumer Disputes Act (SFS 2015:671), and principles about net neutrality and open internet access through Regulation (EU) 2015/2120, as well as a new proposed directive regarding contracts for the supply of digital content.

Sector-specific legislation

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

There is a wide variety of sector-specific legislation in Sweden that concern both private and public actors. There is no legislation that covers cloud computing in particular but these services often fall within the scope of the legislation depending on the sector of operation. Some significant legislation concerns matters of national security in the Security Protection Act (SFS 2018:585), with specific requirements of, for instance, information security and access to information. The Security Protection Act entered into force on 1 April 2019 and is more stringent than its predecessor from 1996.

Cloud companies competing in providing services for public institutions are covered by the Swedish legislation on public procurement, inter alia, the Public Procurement Act (SFS 2016:1145). Public agencies are encouraged by the Swedish Civil Contingencies Agency to use private or partner clouds to be able to provide the necessary security.

There is specific regulation for the processing of personal data in, among others, the health and finance sectors of relevance for transactions in these sectors. In the health sector, personal data is governed by the GDPR supplemented by the Patient Data Act (SFS 2008:355). The legislation in the finance sector, most significantly the Banking and Finance Business Act (SFS 2004:297), is complemented by regulations from the Financial Supervisory Authority, including, inter alia, rules regarding outsourcing and information security as well as the European Banking Association guidelines on outsourcing.

Other sector-specific legislation that is worth noting includes the energy and telecommunications sectors. For private actors, there are no sector-specific requirements regarding cloud service infrastructure besides the above-mentioned requirements in the Act on Information security for vital societal functions and digital services and careful assessments regarding privacy and IT security.

Insolvency laws

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

There is no specific insolvency legislation that applies to cloud computing in Sweden, but the standard legal framework for insolvency apply, notably the Bankruptcy Act (SFS 1987:672), the Enforcement Code (SFS 1981:774) and general Swedish principles of property law. For movable property, the right to property is, in general, decided by who is in possession of the property. For intellectual property, the right to the property is instead decided from what is stipulated by contract.

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.

As of 25 May 2018, the GDPR is the principal legislation governing data protection in relation to cloud computing in Sweden. The GDPR is supplemented by the Data Protection Act (SFS 2018:218) and various sector-specific legislation.

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)?

Usually, the supplier's standard cloud computing contract is applied. Given the bargaining power of the customer, the cloud computing contract may, in rare cases, be based on the customer's standard template, in particular, when the supplier is a local cloud provider. Notwithstanding the above, for certain areas of the cloud computing contract, the suppliers, including international cloud providers, have become more recipient towards implementing customer requirements in the contract. This relates in particular to regulatory requirements, such as requirements deriving from privacy legislation and regulations, requirements on public sector entities and financial regulations.

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?

As cloud computing contracts are often drafted on the basis of the supplier's standard cloud computing contract, governing law will, in many cases, be the law that applies where the supplier's business is based, such as the laws of Ireland or the US. However, you may also find contracts that are governed by Swedish law, in particular from local Swedish cloud suppliers, but also larger international enterprises that have opened up local Swedish entities.

For data privacy, Swedish law will typically apply, in particular since this is a regulatory requirement from the Swedish DPA or at least that was the case prior to the GDPR. As to jurisdiction, principles corresponding with those above would normally apply. In most Swedish B2B contracts, arbitration is used as a method of dispute resolution and this would typically also apply to cloud computing contracts. Ultimately, the choice of rules for dispute resolution as well as governing law and jurisdiction would be the result of the parties' negotiations. Many of the larger cloud service providers will not accept that the agreement will be governed by Swedish law. The enforceability of a cloud service contract is, however, uncertain as there is very limited case law regarding this matter.

Cross-border issues are mostly discussed in respect of data privacy and secrecy. Data privacy cross-border issues are usually regulated through the use of the standard contractual clauses decided by the EU Commission on 5 February 2010 (2010/87/EU) that supplement the cloud computing contract to allow transfer of personal data outside the EEA. Many cloud service providers are reluctant to provide a guarantee that data will not be processed outside the EU and EEA even if they may commit to mainly use data centres within the EEA as their main facilities for the services. The newly adopted US Cloud Act, giving US authorities a right of access to data that is stored by US cloud service providers worldwide, is likely to add to the complex landscape.

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?

Commercial terms of service and acceptable use are commonly agreed on the basis of the supplier's standard cloud computing contract. Price model and payment terms vary depending on the services offered, however, services are commonly purchased as subscriptions and invoiced in advance. Provided that payment is overdue, the supplier may reserve the right to suspend the services immediately, however, sometimes excluding cases where payment is withheld in good faith. Principles for acceptable use commonly include customary restrictions, such as prohibition against redistribution of the services, use of the services for provision of outsourcing services and transmission of infringing material or malicious code.

As to variation, the supplier's standard cloud computing contract will, in many cases, include the unilateral right for the supplier to change the services, including the functionality and security. Such provisions may often be the subject of negotiations between the parties, for example, when the customer is a regulated entity and the provisions are in violation of the regulatory requirements applicable to the customer.

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?

In terms of data, cloud computing contracts have in recent years been greatly influenced by the statements and decisions of the Swedish DPA regarding the processing of personal data by cloud computing suppliers. These statements and decisions prescribe, among other things, that the customer must ensure that:

- a sufficient data processor agreement is entered into with the supplier;
- the supplier is not allowed to independently process personal data but only in accordance with the customer's instructions;
- the contract stipulates that Swedish law applies as regards the processing of personal data; and
- the customer is informed of all sub-processors involved in the processing of personal data type of services and the location of such sub-processors.

In addition, the customer should ensure that it is entitled to perform audits for the purpose of ascertaining the supplier's compliance with the customer's requirements on the processing and that a process for exit of the agreement is established, which safeguards that the supplier will not process the personal data post termination of the contract.

Moreover, the customer is, as a general rule, obligated to perform a legality assessment and risk and vulnerability analysis prior to entering into the cloud computing contract. The purpose of the legality assessment is to determine whether the supplier's processing of personal data under the cloud computing contract will be allowed under the data protection legislation. This includes measures such as ensuring that a data processor agreement is entered into, an assessment regarding cross-border transfers and any security measures necessary. The purpose of the risk and vulnerability analysis is to assess whether it is possible to assign the processing of personal data to the supplier and determine appropriate security levels and necessary measures that need to be taken in the light of the integrity risks involved.

Following the entering into force of the GDPR, it is currently not clear whether the above principles will be upheld by the Swedish DPA.

Confidentiality provisions are commonly mutual.

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?

Since the cloud computing contract in many cases is based on the supplier's standard contract, the supplier's warranties are normally limited. A typical warranty would imply that the services are materially consistent with the documentation, and that the supplier will not materially change the functionality of the services or the security of the services. Ultimately, the warranties may be subject to negotiation between the parties.

Limitation of liability is often mutual with a cap and excluding indirect and consequential damages. There is normally a carve-out for liability for death and personal injury and damages caused by intent or gross negligence. In some agreements, liability for breach of confidentiality is uncapped but with a carveout for loss of customer data entered into the cloud services, which instead falls under the general liability in the agreement.

The supplier would normally provide indemnities for intellectual property rights (IPR) infringements caused by the proper use of the services and, correspondingly, the customer would provide for the IPR infringements caused by the proper use of customer data. You may also find other types of indemnities (eg, in case of violation of applicable law or customers' misuse of the services).

Service levels is a typical area where the cloud computing contracts are less flexible and the customer will in many cases have to accept the supplier's standard SLAs. Penalties and similar possible remedies in the event of non-fulfilment of the SLAs are often limited to fairly low amounts and are sometimes a customer's sole remedy for such non-fulfilment.

Business continuity and disaster recovery plans could be necessary to implement as a result of the risk and vulnerability analysis performed by the customer prior to entering into the cloud computing contract and this would also normally be required by customers that are regulated entities.

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?

The supplier generally reserves the IPR to the services and non-customer-specific content, whereas the customer reserves the IPR to customer data. Customary consequences of infringement of IPR normally apply (ie, modification of the services so that they are no longer infringing, obtaining a licence for the customer's continued use of the services or, ultimately, termination of subscription and refund of licence costs). The customer is often undertaking to indemnify the supplier for any claims made towards the supplier due to the content of the customer data entered into the services.

Typical terms covering termination

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

Either party will typically have the right to terminate the cloud computing contract in case of material breach of the contract by the other party. Additionally, the customer often has the right to terminate the contract in cases where the supplier appoints a sub-processor that the customer on objective grounds refuses to accept. Following termination of the contract, the supplier will no longer have a right to process personal data for which the customer is the controller; however, the supplier is usually allowed a certain period of time to remove such data (up to 180 days are often seen, but it remains to be seen whether this period will change given the GDPR).

The supplier may offer migration services on a time and material basis.

Employment law considerations

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

The Acquired Rights Directive 2001/23/EC would (at least in principle) apply to a business customer entering into a cloud computing contract, provided that the cloud computing services are deemed to be outsourcing.

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 are subject to the taxation rules generally applicable to companies in Sweden. An international cloud computing company providing services to Swedish customers may be subject to Swedish taxation, provided it can be held to have a permanent establishment in Sweden. Subject to the nature of the payment under the cloud computing agreement, withholding tax issues may arise that need to be addressed in the cloud computing agreement.

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.

VAT (25 per cent) will be imposed on provision of cloud computing services from within Sweden. In respect of cloud computing services provided within the EU, a reverse charge will, as a general rule, apply. Specific rules apply for cloud computing services provided from outside the EU.

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.

There is limited case law in Sweden regarding the use of cloud computing. Most case law is based on disputes regarding public procurements. In one notable case from the Administrative Court in 2014, the Court found that there had been shortcomings in a Swedish municipality's agreement with Google regarding the use of cloud services by a public school.

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?

eSAm is an organisation consisting of 23 Swedish authorities and the Swedish Association of Local Authorities and Regions. In October 2018,

eSam issued a statement in which eSam urged public authorities to exercise caution when contracting with suppliers whose ownership or other circumstances may mean the supplier is bound to comply with the laws of a foreign country and that the foreign law forces the supplier to disclose confidential information without there being a legal basis for the disclosure under Swedish law. The US Cloud Act is named as an example of foreign law that obliges a supplier to disclose confidential information.

According to the same statement, caution shall also be exercised if the ownership of the supplier or the geographical location of the supplier's tool are such that there is reason to question the protection of human rights (eg, the protection of private life) or safeguard the public interest (eg, state security). This essentially means that a supplier that is bound by foreign law may contribute to confidential information being disclosed and that this circumstance must be considered when a cloud service is potentially implemented by a public authority.

eSam's statement has been supported by the Swedish Association of Local Authorities and Regions, which also points out that there is a need to conduct a broader analysis prior to a local authority or region deciding to implement a cloud service. The analysis shall include a comparison against the current IT environment and its capacity and several questions shall be answered in regard to, inter alia, the safety, risk and legal requirements of the use of cloud services.

The conclusions are also supported by the central purchasing centre at the Legal, Financial and Administrative Services Agency in a pre-study that was published in February 2019.

In the light of the position taken by eSam and the Swedish Association of Local Authorities and Regions, it can be assumed that contracts with public authorities will take longer to negotiate and that there will be detailed discussions between the parties so the authority can make a thorough analysis and well-founded decision on whether or not to implement cloud services.

Peter Nordbeck
peter.nordbeck@delphi.se

Dahae Roland
dahae.roland@delphi.se

Mäster Samuelsgatan 17
PO Box 1432
111 84 Stockholm
Sweden
Tel: +46 8 677 54 00
Fax: +46 8 20 18 84
www.delphi.se

Switzerland

Jonas Bornhauser*
Bär & Karrer Ltd

MARKET OVERVIEW

Kinds of transaction

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

Cloud computing (and anything-as-a-service (XaaS)) continues to be one of the most important trends in the Swiss IT sector. Although most of the cloud solutions are still deployed in-house (besides traditional outsourcing and managed services), software-as-a-service (SaaS), in particular, is becoming more and more important as a procurement model. Cloud computing is now available for most of the areas of application (ie, including, besides SaaS, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and backend-as-a-service (BaaS)). Private clouds are most commonly used (63 per cent), public clouds and hybrid clouds are on a par with 28 per cent each, although hybrid scenarios continue to gain in popularity as companies are seeking to build an IT services mix based on individual preferences. In this regard, the security of companies' data and cloud providers' data centres as well as a high availability of cloud services play an important role.

EveryWare AG acquired 100 per cent of the shares in the Zurich-domiciled iSource AG as of 1 January 2018. Both companies operate as cloud and IT service providers for medium-sized business customers.

Active global providers

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

The international cloud providers are Amazon, Google, SAP, IBM and Oracle. Microsoft was expected to provide cloud services as of 2019.

Active local providers

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

The leading national cloud providers include myfactory, bexio and ABACUS. Such providers mainly provide SaaS – and, in particular, SaaS enterprise resource planning (ERP) and unified-communication-as-a-service – to private (small and medium-sized) businesses. These providers operate private as well as public or on-premise clouds.

Market size

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

The software market in Switzerland is undergoing substantial changes due to the rising importance of 'as-a-service' offerings. Such services do not only transform the market but also buying patterns. It must, however, be noted that despite SaaS being the fastest-growing segment at the moment, market shares are still limited in relation to on-premises solutions (in particular, software). It appears the latter will remain important for the foreseeable future.

The total market volume of managed private clouds in Switzerland in 2016 was around 440 million Swiss francs and the public cloud market is reported to be around 810 million Swiss francs. In both sectors, SaaS account for significantly more than 50 per cent of the market volume (58.7 per cent private cloud and 81.1 per cent public cloud). The entire market for conventional hardware, software and IT services amounts to more than 27 billion Swiss francs.

Impact studies

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

See, for example, the study 'ISG Provider Lens Germany 2017 – Cloud Transformation/Operation Services & XaaS' from ISG/Experton Group, a global market research company, in which ISG/Experton takes a close look at the cloud market in Switzerland (accessible online at: http://research.isg-one.de/research/studien/isg-provider-lens-germany-2017-cloud-transformationoperation-services-xaas/ergebnisse-ch.html?L=0, the study has been conducted and published for the fourth time).

In addition, the eCH Cloud Computing Group (www.egovernment.ch/en/umsetzung/e-government-schweiz-2008-2015/cloud-computing-schweiz/) has been conducting researches and studying the cloud computing sector since the end of 2014 (the respective papers are accessible online at: www.egovernment.ch/de/umsetzung/e-government-schweiz-2008-2015/cloud-computing-schweiz).

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?

A strategy on cloud computing has been developed by the Swiss Federal Strategy Unit for Information Technology (FSUIT) together with experts from the Confederation, the cantons, the communes, enterprises affiliated with the Confederation and the private sector, and was adopted by the eGovernment Steering Committee on 25 October 2012. The strategy serves to promote both the responsible use of cloud services and the offering of cloud solutions for authorities at all government levels (the respective paper is accessible online at: www.egovernment.ch/de/umsetzung/e-government-schweiz-2008-2015/cloud-computing-schweiz).

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?

No, Switzerland has not (yet) introduced specific regulations for cloud computing. The applicable laws, ordinances and regulations were usually enacted at a time when cloud computing, its possibilities and risks were unknown. According to the above-mentioned strategy on cloud computing (see question 6), the authorities, in cooperation with associations and interest group, must identify necessary adjustments with regard to the current legislation. However, as of today, no cloud-specific regulation has been proposed by the said parties.

Governing legislation

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

No, there are no legal provisions in Switzerland that would (directly or indirectly) prohibit, restrict or otherwise govern, cloud computing, onshore or offshore.

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

Where the customer of a cloud services provider is subject to compliance (eg, national and international stock exchange regulations, obligations in connection with accounting regulations, document retention obligations and audit rights of authorities, etc) or contractual obligations as regards third parties (eg, licence restrictions concerning the use of software and confidentiality obligations), respective obligations must be regulated in the contracts with the cloud services provider which indirectly is obliged to comply with the regulations and obligations. This also applies to compliance with data protection regulations that are imposed on the customers of cloud service providers.

In addition, on 18 March 2016, the Swiss parliament adopted the revised Federal Act on the Surveillance of Mail and Telecommunication Traffic (BÜPF). This act entered into force on 1 March 2018. The revised statute's objective is to improve criminal investigations if telecommunication services are involved. The revised statute is expected to apply also to cloud services providers since they qualify as providers of derived communication services that permit one-way or multiple-way communication. Providers of email services, of chat rooms, of platforms, such as Facebook, that permit communication as well as providers of platforms where documents can be uploaded (for example, Google Docs) are, for example, deemed providers of derived communication services. It is expected that the statute and the respective duties may not be enforced upon non-Swiss domiciled companies, that is, probably most of the providers of such derived communication services. Providers of derived communication (eg, cloud service providers) are obliged to tolerate surveillance measures and, upon request, permit access to their data processing systems. Furthermore, if available, they must disclose the telecommunication 'marginal data'. However, the BÜPF does not impose an obligation to store such data during six months on providers of derived communication (as is the case with regard to telecommunication service providers). Moreover, they are under no obligation to identify their customers.

Breach of laws

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

Unless a conduct is covered by another criminal law provision, non-compliance may result in a fine of up to 100,000 Swiss francs in the following cases:

- non-adherence to a request of the surveillance office; and
- disclosure of a confidential surveillance ordered by the surveillance office.

In addition, the breach of confidentiality obligations, in particular, of the business secrecy (article 162, the Swiss Criminal Code) and the banking secrecy (article 47, the Banking Act) may be sentenced to imprisonment (not exceeding three years) or a fine.

Consumer protection measures

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

The distinction between business-to-business (B2B) and business-to consumer (B2C) transactions is not significant in Switzerland. In particular, no separate body of laws or rules for B2B deals exist but, for B2C contracts, some restrictions apply in regard to consumer protection (see the following paragraph). However, Swiss law does not provide for an equivalent to EU customers' mandatory withdrawal rights set forth in the Directive 97/7/EC on the protection of consumers in respect of distance contracts (Distance Selling Directive) for online sales.

According to the Swiss Federal Private International Law Act (PILA), for disputes arising out of in connection with consumer contracts, the Swiss courts of the consumer's domicile or ordinary residence or of the offeror's (cloud provider's) domicile or ordinary residence have jurisdiction, at the discretion of the consumer. Such place of jurisdiction is mandatory and cannot be waived in advance. The cloud provider can, however, only take civil action against the consumer at the consumer's domicile or ordinary residence or the place of performance. Consumer contracts are defined as contracts for goods and services that are for current personal or family consumption and are not connected with the professional or business activity of the consumer.

Furthermore, regarding consumer contracts, the choice of law is excluded, meaning that they are governed by the law of the state of the consumer's ordinary residence in any of the following instances:

- the supplier received the order in that state;
- the contract was entered into after an offer or advertisement in that state and the consumer performed the acts required to enter into the contract in his or her state; and
- the consumer was induced by the supplier (cloud provider) to go abroad for the purpose of delivering the order.

Entering into business contracts online with a Swiss consumer will, in most cases, fall under the first two groups above. Consequently, the contracts cloud providers enter into with Swiss consumers concluded by electronic means are generally governed by Swiss law.

Sector-specific legislation

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

There is no sector-specific legislation or regulation that applies to cloud computing transactions in Switzerland. Sector-specific laws, however, indirectly apply to cloud computing transactions. In particular, highly sensitive data such as data on health, data subject to attorney–client confidentiality or bank client data are subject to special legal conditions regarding confidentiality, data protection and data security. When data is collected in clouds, special information and due diligence obligations must be respected depending on the type of data that is collected or processed and the actual locations of the cloud data centres.

Insolvency laws

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

Lacking specific insolvency laws for internet providers (including cloud service providers), the general Swiss insolvency laws apply according to which, with the opening of bankruptcy proceedings, claims that are not for a sum of money are converted into a monetary claim of corresponding value. The bankruptcy administration, however, would have the right in the debtor's (cloud provider's) stead to fulfil synallagmatic contracts that had only partly been fulfilled at the time of the opening of the bankruptcy. However, given that the bankruptcy administration is not qualified to provide cloud services, cloud computing contracts are usually terminated if bankruptcy proceedings open. In such cases, a creditor may only request segregation of items (from the bankrupt estate), such as its data, that are the property of the creditor but are in possession of the debtor.

However, according to the prevailing legal doctrine, the Swiss Federal Supreme Court and the practice of the debt enforcement and bankruptcy agencies, such segregation can principally only be claimed for physical objects but not for non-physical ones, such as electronic data. A customer may therefore currently only request segregation if the cloud computing provider is in possession of a separate data carrier that is owned by the customer. For the time being, the customer should therefore be able to continue its operations in the case of the provider's insolvency (eg, backups, etc).

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.

The processing of personal data may only be assigned by an entity to a cloud service provider (B2B) based on an outsourcing agreement, if:

- the data is processed only in the manner permitted for the instructing party itself; and
- it is not prohibited by a statutory or contractual duty of confidentiality.

In addition, the assigning entity must further ensure, that the cloud service provider guarantees data security. In particular, the personal integrity of the data subject must be protected through adequate technical and organisational measures against unauthorised or accidental destruction, accidental loss, technical faults, forgery, theft or unlawful use, unauthorised alteration, copying, access or other unauthorised processing (see article 7, DPA and article 8 et seq, Swiss Data Protection Ordinance). Additionally, if cloud computing services involve disclosures of personal data abroad, the specific requirements for cross-border data flows must be complied with (see article 6, DPA), which are largely aligned with the ones of the GDPR. Furthermore, despite the assignment of the data processing to cloud service providers, the assigning entity remains under an obligation to provide the information requested by one of its customers. The cloud provider is only obliged to provide information if it does not disclose the identity of the assigning entity, that is, the controller, or if the controller is not domiciled in Switzerland (see article 8, DPA).

A Swiss-domiciled cloud service provider not established in the EU may further fall within the scope of GDPR with respect to EU/EEA resident natural persons:

- if it is processing the personal data of such persons; and
- if the processing activities are related to the intentional, active offering of goods or services to the EU/EEA resident persons.

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)?

Cloud computing contracts may comprise various services containing elements of software licence agreements, lease agreements, service level agreements, hardware and software support agreements, data storage agreements and data transmission agreements.

Agreements concerning the provision of IaaS may usually be qualifies as lease agreements or at least as special contracts with substantial lease elements. However, processing ability does not form part of a typical lease contract. It qualifies rather as a mandate agreement (article 397 et seq) or, depending on the specifications of the contract, as a contract for works in accordance with article 363 et seq.

Agreements concerning the provision of PaaS, SaaS or XaaS are usually deemed special contracts if the deployed hardware is used by means of a virtual server. Such special contracts comprise lease and service contract elements, and, depending on the services to be rendered, contract for work elements.

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?

Swiss cloud service providers usually insist that the cloud computing contracts they enter into are governed by Swiss law (under exclusion of the United Nations Convention on Contracts for the International Sale Goods, 11 April 1980, and other international treaties). The same applies with regard to the place of jurisdiction (Switzerland).

Careful attention must be given to dispute resolution mechanisms. Time is often crucial and the customer should ensure that he or she can obtain fast resolution against the cloud service provider if need be.

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?

The general terms and conditions of Swiss B2B public cloud computing providers typically contain the following terms:

- rights to use the software provided by the provider;
- use restrictions:

    - use of the functionalities of the software exclusively according to the specifications and the licensing terms as well as within the scope of the cloud service provided by the provider; and
    - prohibition to make any changes to the software (eg, by further developing the software);
- acceptable use policy:
    - customer to assume the sole responsibility for the content of the data that is being processed in connection with the use of the cloud services; and
    - customer to indemnify the provider against any third-party claims resulting from illegal use of the cloud services;
- security:
    - technical, personnel and organisational security measures to be taken by provider; and
- requirements concerning standardisation and compatibility of technical systems;
- service levels:
    - if specific parameters relating to the availability of the cloud services have been agreed upon, the B2B public cloud computing contract usually sets out the legal consequences of deviations from the services, which are:
        - requirements concerning data backup, return, disaster recovery; and
        - requirements concerning data protection, security and audit rights;
- remuneration:
    - customer may usually choose between different price metrics; and
- limitation of liability:
    - liability usually only for gross negligence and unlawful intent; or
    - if liability is only for mere negligence then limitation of the amount for which a party may be sued.

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?

Since data that is the object of the cloud computing agreement may include sensitive information (eg, business and trade secrets or patient information), cloud computing agreements must also address the confidential nature of data stored with the cloud service provider and the consequences of a breach of the confidentiality obligation.

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 typical terms in this context are:
- service availability;
- asssurance of compliance with data protection regulations;
- guarantee of data integrity, data security, etc;
- implementation of high security standards (encryption, access management, monitoring, telecommunication connections, etc);
- backup scenarios;
- backup of data;
- audit rights to verify compliance with data protection regulations;
- correct and necessary labelling for the identification of dedicated (ie, customer owned) IT infrastructure in the event of bankruptcy (unless the customer explicitly states other wishes);
- conclusion of insurance solutions for data stock/integrity; and
- implementation of regular checks of data security and integrity.

The fact that the cloud service provider can have access to important business data of the customer because the data is located on its infrastructure must be reflected accordingly in the scope and amount of liability. A corresponding service level agreement for business-critical services from the cloud should be part of the cloud computing contract. The same applies to contractual penalties, in particular in the event of breaches of data protection regulations, service-level agreements and confidentiality undertakings.

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?

The cloud service providers usually grant the customer the licence rights to use the required software applications within the framework of the cloud contract, either for the subscription of IaaS, SaaS or XaaS. However, updates or upgrades, release management and so on are the responsibility of the cloud service provider, since the customer has neither licence and maintenance contracts with the corresponding software suppliers, nor do they have the necessary access rights to perform such work.

Typical terms covering termination

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

If a Swiss court qualifies a cloud computing agreement or the substantial parts thereof as mandate agreement in accordance with article 394 et seq, the Swiss Code of Obligation, such an agreement may be terminated by either party without cause at any time with immediate effect. This termination right (article 404, the Swiss Code of Obligation) is mandatory and cannot be validly excluded. However, if termination is effected at an improper time, the party terminating is liable to the other party for the damages caused. Outside the scope of article 404, the parties are free to agree on the contract term and termination rights. However, the tendency is that the customers do not want to enter into long-term agreements with cloud service providers so they can have flexibility to swiftly change the provider.

Cloud computing agreements usually contain termination provisions for both ordinary and extraordinary circumstances and include detailed exit and post-termination assistance provisions. Appropriate notice periods allow the parties to transfer the outsourced services to a third-party provider or take them back in-house.

Employment law considerations

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

The parties to a cloud services agreement should consider whether the agreement may result in the transfer of a business unit and, therefore, the automatic transfer of the customer's employees employed with the business unit to the cloud service provider.

TAXATION

Applicable tax rules

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

A cloud computing company established with its domicile (and place of effective management) in Switzerland is generally subject to unlimited Swiss profit and capital tax (applicable rates vary, depending on the canton of domicile) on its full profit or taxable capital, potentially subject to an international tax allocation in the specific case (eg, generally no taxation right for profit derived from a permanent establishment (PE) abroad) and depending on applicable double taxation treaties. A stamp issuance duty is levied on the creation or increase of the nominal value of shares in a Swiss company, on the amount of share capital or share premium exceeding a once exempt amount of 1 million Swiss francs.

A cloud computing company with its domicile abroad may have a PE in Switzerland and hence is subject to Swiss profit/capital tax (applicable rates vary, depending on the location of the PE) if it has a fixed place of business in Switzerland in which all or a part of the business activity of the enterprise is carried out. The tax liability in this case is in principle limited to the profit/capital to be allocated to the PE. There is currently no guidance published by the Swiss tax authorities based on what circumstances a foreign cloud computing service provider may create a PE in Switzerland. A case-by-case assessment is required and obtaining a tax ruling would be recommended.

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 qualify as an electronic supply of services in the sense of the Swiss VAT Act and are taxable at the ordinary rate of currently 7.7 per cent. The determination of the place of supply follows the place-of-receipt principle.

A Swiss company offering such services mandatorily needs to register for Swiss VAT and subsequently charge Swiss VAT on the services in case its annual turnover from taxable services in Switzerland and abroad exceeds 100,000 Swiss francs (below this threshold, a voluntary Swiss VAT registration generally is possible).

Cloud computing services imported into Switzerland are subject to reverse charge at the level of a Swiss VAT-registered recipient (for non-VAT-registered recipients, no reverse charge applies). To the extent a foreign company provides respective services to Swiss non-VAT-registered recipients, the company needs to mandatorily register for Swiss VAT (and subsequently charge VAT on the services) in case its annual turnover from taxable services in Switzerland and abroad exceeds 100,000 Swiss francs.

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.

None to date.

Jonas Bornhauser
jonas.bornhauser@baerkarrer.ch

Brandschenkestrasse 90
8002 Zurich
Switzerland
Tel: +41 58 261 50 00
Fax: +41 58 261 50 01
www.baerkarrer.ch

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?

No update at this time.

* *The information in this chapter is correct as at October 2018.*

United Kingdom

Mark Lewis*

Bryan Cave Leighton Paisner LLP

MARKET OVERVIEW

Kinds of transaction

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

As a G7 economy with mature IT and related services markets, the UK is one of the most important global markets for cloud computing. According to Gartner, judged by cloud spending rates and growth, the UK is among the fastest cloud adopters globally, ranking behind the USA (the world leader in cloud adoption since 2015) and Canada: https://www.gartner.com/smarterwithgartner/cloud-adoption-where-does-your-country-rank/. In its 2018 BSA Global Cloud Computing Scorecard (the latest version since first publication in 2012 and claimed to be the only global report to rank countries' preparedness for the adoption and growth of cloud computing services), BSA|The Software Alliance ranks the UK at fourth after Germany, Japan and the USA. To account for the difference in the UK's standing in these two reports, it is worth explaining that the BSA Global Cloud Computing Scorecard is based on a methodology that emphasises policy areas that 'matter most to cloud computing', such as data protection and privacy laws, cybersecurity regimes and intellectual property protection (ie, the effectiveness of the legal and regulatory environment for cloud computing). And it also applies a test of IT infrastructure readiness, in particular access to broadband: https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf. Other market analysts, such as MarketsandMarkets™ (https://www.marketsandmarkets.com/), observe that successful implementation of the UK's National Broadband Plan has resulted in faster mobile data connection speeds in the UK, which in turn has facilitated the more rapid adoption of cloud services in the UK.

Using the US National Institute of Standards and Technology (NIST) definition of cloud computing (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf), there is extensive use of the three NIST service models: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS), referred to below as 'service models'. Of the four NIST deployment models (private cloud, community cloud, public cloud and hybrid cloud (deployment models)), private, public and hybrid clouds are widely adopted. Community clouds are also used, though apparently less regularly.

As part of the UK's cloud business ecosystem, there are cloud service brokers (providers who aggregate several different cloud services to provide a unified offering to a customer) and cloud exchanges (providers that offer direct connections between several cloud platforms, enabling their customers access to and portability among separate cloud platforms, without their data passing through the internet). 'Cloudbursting' – in the context of the hybrid deployment model, with customers moving specific processes running in-house to public cloud services to provide greater capacity – has become more common.

A notable feature of the UK market is the adoption by central and local government of cloud computing. In 2012, the UK government introduced the G-Cloud, which enables government departments and state agencies to buy and deploy cloud services from pre-approved vendors, which include some of the biggest cloud providers, for example Amazon Web Services (AWS) (http://searchcloudcomputing.techtarget.com/definition/G-cloud-government-cloud). In February 2017, the UK government reaffirmed the Government Cloud First Policy, under which public sector organisations must consider and evaluate potential public cloud as a deployment model, before considering any other IT option. Cloud First has been mandatory for central government departments and agencies, but has been strongly recommended to the wider UK public sector: www.gov.uk/guidance/government-cloud-first-policy. For the origins of this important cloud initiative, see the UK government's 2011 paper, Government Cloud Strategy, at: www.gov.uk/government/publications/government-cloud-strategy. Recent research has shown that 78 per cent of UK public sector organisations are using some form of cloud-based service, compared with only 38 per cent in 2010 (www.outsourcery.co.uk/about-us/news/public-sector-cloud-adoption-soaring/). However, although adoption of cloud services by UK local government still lags behind central government's rate of deployment, the adoption rate at local government level is apparently steadily increasing.

In May 2019, it was reported in the UK technology sector media that the UK government's Cloud First policy is under review and that it is likely to be replaced by an updated approach that reflects the growing demand for hybrid cloud deployment in the public sector: https://www.computerweekly.com/news/252463001/Government-cloud-first-policy-under-review-by-CCS-and-GDS.

With the UK being one of the most advanced global markets for cloud computing, there is a sizeable business ecosystem serving the primary market, for example, in data centres.

Active global providers

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

All are active in the UK, including (as a small sample):

- Accenture;
- Adobe;
- AWS;
- Avaya;
- Cisco;
- Citrix;
- Dell EMC;
- Dropbox;
- Equinix;

- Facebook;
- Google;
- Huawei;
- IBM;
- Interoute;
- Joyent;
- Kaspersky;
- Microsoft;
- NetApp;
- Oracle;
- Rackspace;
- Red Hat;
- SalesForce;
- SAP;
- SAS;
- Skype;
- Sungard;
- Symantec;
- VMware; and
- Workday.

(See www.cloudpro.co.uk/providers.)

Active local providers

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

The following is a small, illustrative, selection by service segment.

- server, storage and infrastructure: RedstoneConnect, ElasticHosts, Fasthosts, Flexiant, Memset, and VMhosts;
- managed services: BT, Claranet, Colt, Interoute, iomart, IT Lab, Nasstar, TIG and Webfusion;
- data backup and security: BT, Cloud Direct, iomart, IT Lab, Memset, RedstoneConnect, TIG, UKFast, UK2 and Vodafone;
- hosted desktop: Colt, Nasstar and Vodafone; and
- channel enablement, go-to-market, digitisation and CRM: BCSG and NewVoiceMedia.

(See www.computerweekly.com/tutorial/UK-hosted-desktop-cloud-providers; noting that this study was undertaken in 2010 and that it has not been updated since.) For various cloud services mainly focused on the UK public sector, there is UKCloud: https://ukcloud.com/.

Market size

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

See question 1 for the findings of Gartner and BSA|The Software Alliance.

Research undertaken and provided to the author by MarketsandMarkets suggests that in 2019 the UK's cloud computing market will be worth £20.3 billion, rising to £22.8 billion in 2020 (a 12.3 per cent increase from 2019) and £35.1 billion by 2023 (a 73 per cent rise from 2019): source, private research provided to the author by MarketsandMarkets in September 2019, based on primary interviews, secondary literature and MarketsandMarkets analysis.

According to the MarketsandMarkets report referred to above, in 2020 the size of the UK's cloud computing market by service model will be as follows: SaaS £14.3 billion; PaaS £2.1 billion; and IaaS £6.4 billion.

The same MarketsandMarkets report forecasts that, in 2020, the size of the UK's cloud computing market for the three main deployment models will be as follows: private cloud £5.1 billion; public cloud £10.9 billion; and hybrid cloud £6.8 billion.

Impact studies

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

Authoritative, specific, recent data on the true size and therefore impact of cloud computing in the UK is hard to find. And such reports are not in the author's experience freely available to the general public, online or otherwise. See the three reports referred to under questions 1 and 4. Of the three, the MarketsandMarkets report referred to above is the most specific and authoritative by reference to the size of the UK cloud market generally, and by reference more specifically to the cloud service and deployment models.

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?

In short, yes. The policy manifests itself in various forms and initiatives, but comprehensive coverage of them is beyond the scope of this chapter.

The starting point is the government's policy paper, UK Digital Strategy 2017, published on 1 March 2017 by the responsible government department, The Department for Digital, Culture, Media & Sport (www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy). The stated core aim of the policy is 'to create a world-leading digital economy that works for everyone. It is part of this government's Plan for Britain, strengthening our economy for the long term as we take advantage of the opportunities that leaving the European Union provides.' (Ministerial foreword, page 2.)

There are seven elements to this policy, together with a framework for action:

- connectivity – building world-class digital infrastructure for the UK;
- digital skills and inclusion – giving everyone access to the digital skills they need;
- the digital sectors – making the UK the best place to start and grow a digital business;
- the wider economy – helping every British business become a digital business;
- a safe and secure cyberspace – making the UK the safest place in the world to live and work online;
- digital government – maintaining the UK government as a world leader in serving its citizens online; and
- data – unlocking the power of data in the UK economy and improving confidence in its use. The paper affirmed the UK's commitment to implementing the General Data Protection Regulation (GDPR) by May 2018 (https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr). Accordingly, the Data Protection Act 2018 came into force on 25 May 2018. The Act incorporates the GDPR into law in the UK and supplements its provisions.

In April 2017, the Digital Economy Act 2017 was enacted to implement the government's digital strategy (www.gov.uk/government/collections/digital-economy-bill-2016 and www.legislation.gov.uk/ukpga/2017/30/contents/enacted). It is clear from the UK's digital strategy, the Digital Economy Act 2017 and examples of government support given directly or indirectly to cloud computing and cloud-enabled organisations (see question 7), that the policy and implementation framework embraces all the cloud service models and deployment models. And, as outlined in question 1, the UK government is a world leader in its deployment of cloud computing through its Government Cloud First Policy.

Incentives

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

Yes. Although in most cases cloud computing is not specifically mentioned, and eligibility for fiscal benefits, funding and other incentives will depend on specific criteria for particular applications and uses of ICT, it is clear that the incentives do extend to cloud computing and individual elements of it.

Broadly, these incentives are directed at start-ups and early-stage companies as well as more mature technology companies. They generally cover: tax incentives for the companies themselves as well as their investors, grant funding, contributions towards running costs and start-up and later-stage corporate development loans.

Specifically, these incentives include the following as a representative sample.

The Seed Enterprise Investment Scheme
Offering tax efficient benefits to investors in return for investment in small and early stage start-up technology businesses in the UK (www.seis.co.uk/about-seis).

The Enterprise Investment Scheme
Also offering tax benefits to investors in technology companies (https://www.gov.uk/guidance/venture-capital-schemes-apply-for-the-enterprise-investment-scheme).

R&D tax credits
Available for both small and medium-sized enterprises (SMEs) and larger companies (at different levels), tax credits for qualifying R&D, which may include subcontractor costs, supporting software and SaaS, and some hardware costs: https://granttree.co.uk/tax-credits/#r&d-tax.

The Patent Box
Enables SMEs and larger companies to apply a lower rate of UK Corporation Tax to profits earned after 1 April 2013 from their patented inventions (www.gov.uk/guidance/corporation-tax-the-patent-box).

Innovation funding
For innovative products, processes or services, funding of between £25,000 and £10 million is available. Innovate UK runs funding competitions for projects led by UK-based companies. As at July 2019, competitions include the opportunity to apply for a share of up to £25 million to deliver 'ambitious' or disruptive R&D innovations that can make a significant impact on the UK economy, and the chance to obtain loans for 'game-changing' innovations with strong commercial potential that will significantly improve the UK economy (www.gov.uk/guidance/innovation-apply-for-a-funding-award and https://apply-for-innovation-funding.service.gov.uk/competition/search).

Regional growth funds
Grants and loans of up to £1 million are available through regional growth funds (RGF) programmes, namely schemes run by national or local organisations that have been awarded RGF funds to offer grants and loans to eligible businesses. The schemes have invested a total of £2.6 billion in eligible businesses since the launch of the RGF in 2010. Each RGF programme will have specific criteria for applications (https://www.gov.uk/guidance/understanding-the-regional-growth-fund).

The British Business Bank and enterprise capital funds
The British Business Bank (TBBB) invests alongside venture capital funds (partners) under a rolling programme. Funding is aimed at smaller UK growth companies. One of TBBB's partners, Notion Capital, invests in enterprise SaaS and other cloud computing businesses. In July 2015, Notion Capital announced a US$120 million fund that would continue to invest in European business-to-business (B2B) high-growth SaaS companies (british-business-bank.co.uk/british-business-bank.co.uk/british-business-bank-partner-notion-capital-launches-new-fund/; www.notioncapital.com/about/; and https://notion.vc/portfolio/filter/sector/cloud-services/).

LEGISLATION AND REGULATION

Recognition of concept

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

Except as mentioned in question 9, no, not specifically.

Governing legislation

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

Yes, in respect of cybersecurity and resilience and cyber incident reporting. The Network and Information Systems Regulations 2018 (www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf), which implement the NIS Directive (2016/1148/ EU), specifically govern a 'cloud computing service', meaning 'a digital service that enables access to a scalable and elastic pool of shareable computing resources': regulation 1(2). Cloud service providers (CSPs) who fall within the definition of a 'relevant digital service provider' (RDSP) must, broadly stated, take appropriate and proportionate technical and organisational measures to prevent and minimise the impact of cyber incidents and related risks to their systems. RDSPs are also required to notify within 72 hours the UK Information Commissioner's Office (ICO, the regulator for these purposes) of any incident that has a substantial impact on the provision of the cloud services. The ICO has a range of enforcement powers, including the right to issue financial penalties for material contraventions, up to a maximum of £17 million. RDSPs were required to register with the ICO by 1 November 2018. There are exceptions for, among others, small or micro businesses.

The ICO has issued a detailed and helpful Guide to the NIS Regulations, which as a first step all CSPs operating in the UK should consult: https://ico.org.uk/for-organisations/the-guide-to-nis/. Included in the Guide are pointers to the cloud services to be governed by the Regulations. The Guide states that PaaS and IaaS service models will be covered, but that SaaS will only be regulated to the extent that the service is 'scalable and elastic' and B2B. Readers are also referred to the UK National Cyber Security Centre's guidance at: www.ncsc.gov.uk/guidance/introduction-nis-directive.

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

In the UK, as business-to-consumer (B2C) and B2B IT services, cloud computing services will – depending on the scope of the services and the circumstances and context of their supply – be subject to the legislation and regulation that apply to all similar IT services. Given the breadth and complexity of the cloud computing business ecosystem in the UK, other participants in the provision of elements of cloud infrastructure and in the cloud supply chain may be subject to that legislation and regulation, too, for example a communications service provider supplying a transmission service enabling the CSP to

communicate with a cloud customer, or the provider of cloud servers to a CSP.

As such (and with applicable B2C cloud computing consumer-protection measures referred to under question 12 and data protection law referred to under question 15), the following are likely to apply to cloud computing (or elements of it) in the UK:

- Digital Economy Act 2017 (www.legislation.gov.uk/ukpga/2017/30/contents/enacted – see question 6);
- Investigatory Powers Act 2016 (as amended) (www.legislation.gov.uk/ukpga/ 2016/25/contents/enacted – interception of communications and retention of communications data, etc);
- EU Dual-Use Regulation 2009, Council Regulation (EC) No 428/2009 (and associated legal amendments) (www.gov.uk/guidance/controls-on-dual-use-goods – regulates the export of dual-use technologies and software);
- Export Control Order 2008: www.legislation.gov.uk/uksi/2008/3231/contents/made – controls on the export of military and certain other technologies and software;
- Communications Act 2003 (www.legislation.gov.uk/ukpga/2003/21/contents – overall regulatory structure and powers for communications and media in the UK, including the regulator, Ofcom);
- Export Control Act 2002 (www.legislation.gov.uk/ukpga/2002/28/contents – controls on the export of, among others, strategic technologies);
- Regulation of Investigatory Powers Act 2000 (www.legislation.gov.uk/ukpga/2000/23/introduction – interception of communications and data retention, etc) as amended; and
- Unfair Contract Terms Act 1977 (www.legislation.gov.uk/ukpga/1977 – makes unenforceable certain terms in B2B contracts that do not satisfy the requirements of 'reasonableness').

The above is not an exhaustive list, and readers should also consider other areas covered by UK legislation and regulation, for example regarding intellectual property rights and employment law, some of which are covered below.

Apart from legal and regulatory enactments, particularly in the context of cloud computing, readers should be aware of various international law enforcement measures under treaty and applicable EU measures that are likely to be relevant. These generally relate to cybercrime, criminal investigations and enforcement, and inter-state mutual legal assistance in criminal matters (MLA). (See, for example: the Council of Europe Convention on Cybercrime 2004, ETS No. 185 at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461&back=5441; and the UK's (then) proposed bilateral ratification of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at www.gov.uk/government/uploads/system/uploads/attachment_data/file/238612/7613.pdf.)

Although beyond the scope of this section, readers will be aware of the extraterritorial impact of the USA PATRIOT Act on cloud services (www.wired.com/insights/2011/12/us-cloud).

To give readers a complete view, the same rules and principles (including as to liability) that apply to consumer and commercial technology-related services contracts under the three UK jurisdictions (England and Wales, Scotland, and Northern Ireland) will apply to cloud computing contracts – again subject to the scope of the services and the circumstances and context of their supply.

Although it is not legislation or public regulation, for the reasons given below, the Cloud Industry Forum Code of Practice for Cloud Service Providers (CIF Code) is relevant. Its stated purpose is 'to bring greater transparency and trust to doing business in the cloud' – for an overview, see www.cloudindustryforum.org/content/code-practice-cloud-service-providers). The CIF Code could influence the choice of CSP by potential customers, whether consumers or commercial organisations. CSPs claiming compliance with the CIF Code and the right to use CIF certification may, for validated infringement, face sanctions by CIF, including publication of CIF's findings on its website and press releases. So, while the CIF Code does not have any public legal effect, it may be normative to the conduct of CSPs and it may influence the choice of CSP by commercial end users and consumers, as well as the public's view of certain CSPs – especially those who have contravened the CIF Code.

Finally, though it too is not legislation or public regulation, the role of the UK Advertising Standards Authority (ASA) is important in the fast-growing cloud services market. The ASA's role is to ensure that all advertisements are 'legal, decent, honest and truthful' (www.asa.org.uk/about-asa-and-cap.html). The ASA publishes codes that it administers and under which it hears and rules on complaints. ASA rulings are published weekly and are 'a transparent record of what is and isn't acceptable' in advertising. The rulings can remain on the ASA website for five years (www.asa.org.uk/codes-and-rulings/rulings.html.) Though ASA rulings do not have any legal effect, an adverse ruling may have significant commercial impact, especially if a business is seen to be disregarding rules designed to protect consumers. And, as a last resort, if advertisers persistently break the ASA codes and are unwilling to change their practices, the ASA states that it can and does refer those advertisers to enforcement agencies – who do have legally enforceable powers and the ability to impose legal sanctions – for further action, for example UK Trading Standards or Ofcom (the communications regulator) (www.asa.org.uk/codes-and-rulings/sanctions.html). It is worth noting that the ASA has in the past considered several specific cloud computing-related advertisements and has found against advertisers (www.asa.org.uk/rulings/jdi-backup-ltd-a14-260786.html, www.asa.org.uk/rulings/jdi-backup-ltd-a13-226451.html; www.asa.org.uk/rulings/jc-inc-a12-215093.html; www.asa.org.uk/rulings/uk-2-ltd-a13-252423.html).

Breach of laws

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

For laws and regulations, the consequences of breach range from contractual unenforceability and civil enforcement remedies to criminal and regulatory fines, penalties and other sanctions. In some situations, company directors and senior executives may face personal sanctions. (For the CIF Code and ASA codes, see question 10.)

Consumer protection measures

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

For B2C cloud computing arrangements, the following main consumer protection measures will apply.

- the Electronic Commerce (EC Directive) Regulations 2002 (www.legislation.gov.uk/uksi/2002/2013/contents/made);
- the Consumer Protection from Unfair Trading Regulations 2008 (www.legislation.gov.uk/uksi/2008/1277/contents/made);
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (www.legislation.gov.uk/uksi/2013/3134/contents/made); and
- the Consumer Rights Act 2015 (www.legislation.gov.uk/ukpga/2015/15/contents/enacted).

Together these cover matters including distance selling, the provision of certain information to consumers, marketing and marketing claims, onerous and unfair contract terms and how they are presented, cancellation rights, 'cooling-off' periods, choice of law and venue for consumer litigation.

Other legislation includes:

- the Financial Services and Markets Act 2000 (www.legislation.gov.uk/ukpga/2000/8/contents (FSMA));
- the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (www.legislation.gov.uk/uksi/2001/544/contents/made); and
- the Consumer Credit Act 1974 (as amended) (www.legislation.gov.uk/ukpga/1974/39).

Together these regulate B2C credit terms, including any form of 'financial accommodation', and specify certain contract terms and restrictions (with sanctions, including legal unenforceability except by court order), the provision of certain kinds of information, the format of that information, 'cooling-off' periods and termination processes.

The above are not exhaustive lists.

The Competition and Markets Authority (CMA), the UK's primary competition and consumer authority, has historically taken a close interest in B2C cloud storage contracts, in particular to see if consumers are being fairly treated when saving and storing their content online. The CMA found that some CSPs were using contract terms and practices that it was concerned could breach consumer protection law ('An open letter to cloud storage providers on complying with consumer law', May 2016, www.gov.uk/government/uploads/system/uploads/attachment_data/file/526355/open-letter-cloud-storage-providers.pdf.) The upshot was that several of the leading B2C cloud storage providers, including Amazon, Apple and Microsoft, voluntarily modified their terms for the benefit of UK consumers (www.gov.uk/government/news/cma-secures-better-deal-for-cloud-storage-users).

Sector-specific legislation

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

The extent (if any) to which UK industry sectoral regulation may apply to cloud computing will require knowledge and the examination of sector-specific legislation, regulations, guidance and regulatory and statutory codes of conduct. In the UK – and with the exception of the NIS Regulations referred to in question 9 and the following example – at the time of writing this chapter there is no regulation that applies specifically or directly to cloud computing as such. Where regulation is found to apply to a cloud computing project, the approval, licence or consent – or at least the informal go-ahead – of a regulator may be required. Common sense and best practice dictate that, where applicable, the regulated entity should consult its regulator as soon as practicable and as fully as possible. This should also be of concern to a CSP expecting to enter a cloud arrangement with a regulated customer.

Only in the UK financial services sector has cloud computing been specifically addressed. Operational resilience, including outsourcing to the cloud, has been identified as a cross-sector priority in the Financial Conduct Authority (FCA),'s annual regulatory business plans for the past several years. The FCA, Bank of England and Prudential Regulation Authority (PRA) issued a joint Discussion Paper (18/4) in July 2018 on operational resilience, which stressed the importance of understanding and mapping important third party providers. Issues identified in the Discussion Paper will be developed into joint policy proposals later in 2019.

In July 2016, the FCA issued its finalised FG 16/5 – 'Guidance for firms outsourcing to the 'cloud' and other third-party IT services' (www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it; www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf (FCA Cloud Guidance)). In July 2018, the FCA Cloud Guidance was modified as mentioned below. While some regulatory objectives are issued by the FCA and the PRA as 'guidance' (as opposed to rules), it would be a foolhardy regulated financial services organisation that disregarded such guidance or diluted it too far in application.

Before outlining the FCA Cloud Guidance, it must be put in its sectoral regulatory context. When financial services organisations (firms) regulated under FSMA (see question 12) by the FCA and PRA engage in any IT, business process or other outsourcing, they must have regard to and, if applicable, comply with, the regulatory guidance and rules governing that outsourcing. The PRA supervises banks, insurance companies, building societies, credit unions and certain large investment entities. The FCA regulates the conduct of business of all financial services organisations within its statutory jurisdiction, including those prudentially supervised by the PRA. Some outsource providers (who, incidentally, are also CSPs) are themselves authorised and regulated by the FCA.

The PRA and FCA rules are complex and their application to outsourcing will depend on the nature of the firm (the outsourcing customer), the financial services and related activities to be outsourced, and the impact of the proposed outsourcing. The main rules and guidance governing outsourcing by regulated firms are contained in the FCA Handbook and PRA Rulebook. There is also more general FCA guidance on outsourcing to meet FSMA compliance. These are the main sources of prudential and operational provisions regulating outsourcing by financial services firms and regulated outsource providers in the UK. There are also specific outsourcing-related obligations on insurance and reinsurance companies under the Solvency II Directive (2009/138/EC) and related subordinate rules and guidelines (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563889385175&uri=CELEX:02009L0138-20190113 and https://www.bankofengland.co.uk/prudential-regulation/key-initiatives/solvency-ii).

The detailed rules governing outsourcing under the PRA Rulebook, FCA Handbook, Solvency II Directive and Solvency 2 Regulations 2015 are beyond the scope of this section. In essence, though, the rules provide for what should be regarded as sensible outsourcing practice, having regard to systemic risk, initial diligence and ongoing operational risk affecting the conduct of regulated business and the interests of business and consumer end-customers, and the needs of the regulators to supervise and intervene if necessary (for a fuller statement, see the FCA Handbook, Systems and Controls (SYSC), chapters, 3, 4, 8, 13 and 14: www.handbook.fca.org.uk/handbook/SYSC/).

The Markets in Financial Instruments Directive (MiFID) II (2014/65/EU), which repealed and recast the MiFID Directive (2004/39/EC) and (largely) entered into force on 3 January 2018, together with the Delegated Regulation (2017/565/EU) (commonly referred to as the MiFID Organisation Regulation or the MiFID Org Regulation), imposes on regulated firms a wide range of conduct of business and organisational requirements. These include requirements relating to outsourcing, as well as more general record keeping and business continuity issues. The FCA handbook was updated to reflect these requirements.

The European Banking Authority (EBA) published finalised Guidelines on Outsourcing Arrangements (EBA Guidelines) on 25 February 2019: https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements. The EBA Guidelines apply from 30 September 2019, and firms must amend existing outsourcing arrangements to comply with the EBA Guidelines by 31 December 2021. They apply to credit institutions and investment firms, as well as to authorised payment institutions and e-money institutions.

The EBA Guidelines are divided into five sections, or Titles: (I) Proportionality: group application and institutional protection schemes (setting out a principle of proportionality in application of the EBA Guidelines, and requiring transparency within groups); (II) Assessment of outsourcing arrangements (defining 'outsourcing' and 'critical or important' functions); (III) Governance framework; (IV) Outsourcing process (setting out aspects to be included in an outsourcing agreement at a minimum for a critical or important function); and (V) Guidelines on outsourcing addressed to competent authorities. The governance framework in Title III requires: a holistic risk management framework, a written outsourcing policy, management of conflicts, business continuity plans, internal audit and a register of information on all outsourcing agreements. EBA Guidelines on internal governance published in March 2018 should also be taken into account.

The EBA Guidelines replace the Committee of European Banking Supervisors Guidelines on Outsourcing published in 2006, and incorporate the EBA Recommendations on Outsourcing to Cloud Service Providers (which were applicable from 1 July 2018). The FCA Cloud Guidance was updated in July 2018, to confirm that the FCA Cloud Guidance does not apply to a bank, building society, designated investment firm or IFPRU investment firm to whom the EBA Recommendations are addressed: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf. The FCA has confirmed that it will keep its Cloud Guidance under review to assess what, if any, changes are required, including as a result of Brexit. In the interests of space, this section now focuses on the FCA Cloud Guidance.

The FCA Cloud Guidance is addressed to such firms (see previous paragraph) 'when outsourcing to the "cloud" and other third party IT services'. As is evident from the FCA Cloud Guidance, for the FCA, not only is cloud computing equivalent to outsourcing in its potential impact on regulated firms, their operations and end-customers, but also it sees the cloud 'as encompassing a range of IT services provided in various formats over the Internet' (paragraph 1.4 FCA Cloud Guidance). Accordingly, the FCA sees no distinction between private, public or hybrid cloud deployment (paragraph 1.4 FCA Cloud Guidance). And it says that '[from] a regulatory perspective, the exact form of the service used does not, in itself, alter the regulatory obligations placed on firms'. So, where a third party (including a CSP) delivers services on behalf of a regulated firm, this is considered outsourcing. Firms therefore need to consider the relevant regulatory obligations and how they comply with them.' (Paragraph 3.3 FCA Cloud Guidance.)

The stated aim of the FCA Cloud Guidance is to facilitate adoption of cloud computing in the regulated financial services sector, recognising the benefits of cloud computing and innovation in the sector. It came about because firms and CSPs had told the FCA that they were unsure about how to apply its Handbook outsourcing rules to the cloud: this uncertainty may have been acting 'as a barrier to firms using the cloud' (paragraph 1.3 FCA Cloud Guidance).

Apart from the regulated firms themselves, the FCA Cloud Guidance is stated to be of interest to third-party IT providers, trade associations and consumer groups, professional advisers and the auditors of regulated firms.

In outline and focusing below on the most important aspects of the FCA Cloud Guidance for cloud computing, the regulated firm in scope of the FCA Cloud Guidance must have regard to the following.

Criticality or materiality of the cloud service

Whether the function being processed under the cloud service is 'critical or important' or 'material' and (for authorised payment institutions and authorised electronic money institutions) if it relates to 'important operational functions'. Each of these terms is defined in the FCA Handbook and the Electronic Money Regulations 2011 (www.legislation.gov.uk/uksi/2011/99/contents/made and Payment Services Regulations 2009: www.legislation.gov.uk/uksi/2009/209/contents/made; paragraph 3.6 FCA Cloud Guidance); and see also the EBA Guidelines section 4, and paragraph 20 of the accompanying EBA Final Report. Overall, if the above kinds of functions are 'outsourced' to the cloud, firms in scope of the FCA Cloud Guidance will have more stringent duties with regard to management of operational risk in the transaction, as will CSPs in enabling firms to comply with their obligations. In addition, firms must notify the FCA when entering into or significantly changing material or critical cloud services arrangements (paragraph 3.7 FCA Cloud Guidance).

In some cases, dual-regulated firms subject to the PRA's preferred resolution strategy will also have to consider resolution arrangements when entering into cloud services projects. These arrangements are designed to ensure continuity in distressed economic circumstances or insolvency to ensure that 'critical economic functions' are maintained (paragraph 3.8 FCA Cloud Guidance and https://www.bankofengland.co.uk/financial-stability/resolution).

Legal and regulatory considerations

These include having a business case or rationale for the decision to outsource to the cloud and the use of one or more CSPs for the delivery of critical or important operational functions, or a material outsourcing; due diligence risk assessment of the proposed project; relative risks of each type of cloud service or deployment model (eg, private versus public cloud); knowing where the CSP service and other relevant locations are situated; and the need to identify all service providers in the cloud supply chain – to ensure that the regulatory requirements are met throughout the supply chain.

Risk management

Including: conducting and documenting a risk assessment of the proposed cloud project; monitoring concentration risk, to avoid too great a dependency on any one CSP; and understanding what action to take if the CSP failed.

International standards

Including: as part of due diligence, assessing the CSP's adherence to accepted international IT and service standards; and applying greater standards of assurance when the functions concerned are critical or important or a material outsourcing.

CSP oversight

Including: clarity about the allocation of responsibilities between the firm and the CSP; the firm having an internal function responsible for the strategic and day-to-day management of the CSP; and ensuring that the firm's staff have sufficient skills and resources to oversee and test the cloud services and properly manage an exit or migration from the existing CSP. In other words, this would mean firms having and retaining specific cloud service management expertise.

Data security

Including: conducting a specific risk assessment; agreeing data residency terms with the CSP, setting out contractually the locations in which the firm's data can be stored, processed and managed; considering how the firm's data will be segregated (for public cloud); assessing the sensitivity of data and how the data will be transmitted, stored and encrypted, where necessary – noting that encryption keys or other forms of authentication must be accessible to the FCA or PRA.

Data protection

Including: continuing compliance with data protection laws. Firms are, of course, required separately to comply with UK data protection law

(now the GDPR, as supplemented by the Data Protection Act 2018). In that sense, though the data protection laws are separate, the FCA Cloud Guidance forms part of the firm's compliance with its duties as a regulated firm. Firms should consider the UK Information Commissioner's guidance concerning the transmission of personal data outside the European Economic Area (EEA).

Effective access to data

'Data' is used here in its widest meaning. Firms should ensure that the cloud computing arrangement has addressed the following: access for the firm, their auditors, the regulators and other competent authorities to the firm's data; contractual ability for the regulators to contact the CSP directly where the firm cannot for any reason disclose the data; ensuring that the data is not stored in jurisdictions that may prevent or inhibit effective access for UK regulators; geopolitical stability as it concerns the data; whether the CSP's jurisdiction provides for data protection; the law enforcement provisions of the relevant jurisdiction or jurisdictions where data is to be processed, for example, whether and how easily the authorities in the CSP's jurisdiction may intervene in accessing the firm's data.

Access to business premises

'Premises' here include head offices and operations centres, but not necessarily data centres. The guidance includes: knowing which CSP or supply chain premises are relevant for the cloud services and effective oversight of them (the FCA recognising that CSPs may have legitimate reasons for limiting access to some sites, eg, data centres); providing for the unrestricted contractual and legal ability for the firm or its auditors to request an onsite visit to the business premises – on reasonable prior notice, except in the case of an emergency or crisis; enabling visits by the financial services regulators or other competent authorities as they deem necessary and required by law or regulation, without any conditions being imposed; having the CSP commit contractually to cooperating with all reasonable requests of the regulators during such visits; affording the regulators the right to observe the provision of the cloud services to the firm or any of its affiliates (although the regulators may commit to minimising disruption to the CSP's operations).

Relationship between service providers

Including: considering how the cloud supply chain is constructed and operates; enabling the firm to review subcontracting and other supply chain arrangements to ensure that they facilitate the firm's compliance with its regulatory requirements, including security, effective access to data and business sites; understanding the roles of CSPs within the supply chain; knowing how a CSP's services will interface with the firm's own systems or other necessary third-party systems (eg, agency banking arrangements for payments).

Change management

Including: ensuring that contractual and operational provision is made for changes to the cloud services; and establishing how changes will be tested.

Continuity and business planning

Including: providing contractually and operationally for appropriate arrangements for the continuity of functions and the ability of the firm to meet its regulatory obligations in the event of an 'unforeseen interruption' of the cloud services; having a plan documenting the continuity, business interruption and recovery arrangements; regular testing of the business continuity plan; and putting in place contractual and operational measures to ensure regulatory access to data in an insolvency or other disruption of the cloud services.

Resolution

This guidance will only apply to certain firms (see 'Criticality or materiality of the cloud service' above). In this context, the main aspect of the resolution and recovery arrangements and the Bank of England's 'stabilisation' powers that will concern firms, CSPs and providers within the cloud supply chain is this: neither financial distress or insolvency leading to resolution, nor the change of ownership or control of the firm following that event, will enable the CSP or a cloud supply chain provider to terminate the contract or the provision of cloud services. Moreover, the CSP and its supply chain may have to provide the cloud services to the resolution successor entity or firm for a transitional period. The CSP (and by implication providers in its supply chain) must agree not to delete, revoke or change the firm's data in the case of resolution.

Exit planning

Including: firms having contractually documented exit plans and termination assistance arrangements to ensure continuity, and these plans being 'fully tested'; firms understanding how they would migrate the cloud services to an alternative CSP and maintain business continuity; contractually requiring the CSP (and by implication its supply chain) to cooperate fully with the firm and the incoming CSP to ensure a smooth transition; the firm understanding how it could and would remove its data from the CSP's systems on exit.

The aim of the FCA Cloud Guidance is to help overcome the barriers created by the perceived regulatory uncertainty in the adoption of cloud computing by UK financial services firms. As the FCA says: 'We see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration, in a manner that complies with our rules.' (Paragraph 1.6 FCA Cloud Guidance.)

The UK banking sector trade body, UK Finance, sponsored the creation of a public cloud computing framework in February 2019. The framework consists of 44 controls, with each control mapped to one of nine domains and one of 11 risks associated with the management of cloud computing as a service. The controls are derived from analysis of UK Finance members' control sets and in collaboration with CSPs, cross-checked for compliance against various industry standards as well as the EBA Guidelines. My own experience and that of my colleagues shows that, despite laudable efforts by the regulators and industry bodies to help firms around financial services regulatory hurdles in adopting the cloud, there are still significant concerns about the compatibility of cloud computing with regulatory compliance. In February 2017, the British Bankers' Association (now UK Finance), identified seven barriers to cloud adoption:

- the regulatory approach to 'important' and 'critical' functions;
- supervision and oversight;
- the risk framework;
- access to CSP sites and services by regulators;
- data residency;
- termination; and
- data breaches and monitoring.

Most of these concerns will be identifiable from the FCA Cloud Guidance summarised above and look likely to remain of concern to the financial services sector in the immediate future.

Insolvency laws

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

There is no specialist insolvency regime for cloud computing. The primary UK insolvency regime is set out in the Insolvency Act 1986 (www.legislation.gov.uk/ukpga/1986/45/contents) and the Insolvency (England and

Wales) Rules 2016 (www.legislation.gov.uk/uksi/2016/1024/contents/made) (both as amended). For an overall guide to the UK insolvency regime, see www.pwc.co.uk/assets/pdf/insolvency-in-brief.pdf.

The rules that govern the insolvency of a CSP or a cloud customer, as well as those governing how corporate insolvencies are managed and disposed of, are complex. And experience in the UK has shown just how difficult it can be for cloud customers when a CSP suffers financial distress and insolvency. In early 2013, UK CSP 2e2 went into administration and subsequently liquidation (http://diginomica.com/2015/01/06/cios-worst-nightmare-cloud-provider-goes-bankrupt/). As a result, UK CSP customers are advised to consider carefully:

- the selection of their CSP;
- ongoing monitoring of the financial robustness of the CSP; and
- the terms of their cloud service contracts, including ownership of the customer's tangible and intangible assets, exit arrangements and data migration where the CSP suffers financial distress or insolvency.

In addition, CSPs and other IT providers operating in the UK need to be aware of legislation that could severely restrict their ability to withdraw service from insolvent customers, terminate supply contracts or demand higher payments for continuity of supply. The legislation overrides conflicting terms in a supply contract – see sections 233 and 233A of the Insolvency Act 1986 (as amended by the Insolvency (Protection of Essential Supplies) Order 2015 (www.legislation.gov.uk/uksi/2015/989/article/2/made). The amendments introduced by the 2015 Order ensure that, like utility services, 'communication services' and other IT supplies will now be treated as essential supplies. 'IT supplies' include a 'supply of goods and services . . . for the purpose of enabling or facilitating anything to be done by electronic means', specifically including computer hardware and software; information, advice and technical assistance in connection with the use of information technology; data storage and processing; and website hosting – in other words, they are wide enough to cover cloud computing services.

The regime prevents suppliers of 'essential supplies' (water, electricity, gas, communication services and other IT supplies) from requiring payment of pre-insolvency charges as a condition of continuing to provide supplies in specified formal insolvency situations. In addition, where a customer enters either administration or a company voluntary arrangement, the regime locks the CSP into the pre-insolvency contract (subject to certain safeguards) to prevent the CSP from terminating supply, terminating the contract or increasing prices.

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.

The main data protection and privacy legislation in the UK comprises the GDPR and the Data Protection Act 2018 (DPA). The DPA is the UK's implementation of the GDPR; although the DPA also supplements the GDPR in certain areas. It is the successor to the previous Data Protection Act 1998. The ICO issued, for organisations rather than members of the public, specific guidance on the use of cloud computing. Although this guidance has not yet been updated to reflect the DPA, the ICO states that it 'still considers the information useful'. At the time of writing, the ICO has confirmed that the guidance will be updated soon.

The following section outlines the likely and most direct impact on cloud computing in the UK of the GDPR and the DPA.

General knowledge of the principles of the GDPR and the terminology used in that legislation is assumed. It is beyond the scope of this section fully to cover the contents and operation of the GDPR. The following focuses on certain elements of the GDPR that are new to data protection law or that have particular significance for cloud computing. This outline is not, therefore, exhaustive. References below to articles are to the articles of the GDPR.

Territorial scope

The GDPR applies to the processing of personal data within the context of the activities of an establishment of a controller or processor in the EU, regardless of whether such processing takes place in the EU or not. Clearly, the GDPR applies to the processing of personal data of a controller or processor in the EU; in addition, draft guidelines from the European Data Protection Board at the time of writing indicate that 'within the context of the activities' is capable of a wider meaning depending on the context itself. This developing area will be of interest to CSPs. The GDPR will also apply to the processing of personal data of data subjects in the EU by data controllers and processors with no EU establishment where the processing relates to offering goods and services (free or for payment) to EU data subjects, or to monitoring the behaviour taking place in the EU of such data subjects (article 3(2)). The GDPR applies, therefore, to CSPs (assuming them to be either processors or controllers) without sites in the EU, if they meet either or both of the above tests. Certain controllers or processors (including CSPs) will have to appoint a local EU representative for legal enforcement purposes (article 27).

Data controllers

Generally – though it should not always be assumed – in B2B cloud computing the customer will be the controller, determining the purposes and means of the processing of personal data (article 4(7)). It will be in the interests of CSPs to ensure that this characterisation continues under the GDPR, as ultimately the controller will be bound by more stringent duties than the processor. The challenge in B2C cloud computing, especially for social media and network services, is how CSPs ensure that their standard public cloud contract terms maintain consumer customers as controllers – if indeed the legislation applies to those consumer contracts at all.

The controller, or cloud customer, will be primarily liable for lawful processing, including implementing appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing is performed in accordance with the GDPR, including ongoing reviews and the updating of those measures (article 24(1)). Cloud customer-controllers must, therefore, be able to demonstrate that processing performed on their behalf by CSPs is compliant, which in turn will mean having to satisfy themselves that CSP contract terms facilitate the controller's obligations.

Controllers should only engage processors who provide sufficient 'guarantees' to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of the GDPR and ensure the rights of data subjects (article 28(1)). This raises important questions for cloud customer due diligence in appointing CSPs. In some cases, for example regulated financial services firms deciding to engage CSPs for their operations, this aspect of the decision will almost certainly have to be documented (see question 13).

The controller may refer to the adherence to approved codes of conduct under article 40 or to approved certification mechanisms under article 42 for the purpose of demonstrating compliance with its GDPR obligations (for the current European Union Agency for Network and Information Security (ENISA) framework see www.enisa.europa.eu/news/enisa-news/enisa-cloud-certification-schemes-metaframework/). We should expect to see the development by CSP industry organisations of cloud-specific codes of conduct and certification mechanisms, for example, the CIF Code referred to under question

10; although such codes and certification mechanisms will have to be approved.

Although article 28 is headed 'Processor', it is clear that some of the obligations it imposes, for example, under article 28(1), are directed to and will be the primary responsibility of controllers. And so it is with article 28(3), which requires not only for there to be a binding contract between the controller and processor governing data processing, but also for that contract to stipulate a range of specific provisions (article 28(3)(a)–(h)), including, for example: that processing will only be in accordance with the controller's documented instructions, including with regard to third country data transfers; confidentiality undertakings by all those authorised to process the data; controls on the engagement of sub-processors (see below); and processor obligations to assist the controller in ensuring compliance under articles 32 to 36 regarding its obligations of data security, pseudonymisation and encryption, data breaches and notifications, and data protection impact assessments. Cloud customers and CSPs must address these requirements in their cloud computing contracts, whether on the CSP's standard contract terms or otherwise. Article 28(8) provides that both regulators and the European Commission may adopt standard contractual clauses (SCCs) covering the requirements of article 28(3); no such clauses have been adopted by the European Commission or the Information Commissioner's Office to date. We should expect that any SCCs adopted will be focused on compliance with the legislation's requirements, and may not be suitable for CSPs or customers wishing to accommodate commercial issues in their drafting.

Processors

As stated above, in B2B cloud computing, the CSP is usually likely to be – and to prefer to be – the entity processing personal data on behalf of the controller, namely the processor: article 4(8). Among the changes to data protection law made by the GDPR is that processors – hence CSPs – are for the first time directly accountable for and liable to data subjects and regulators for infringements. Aside from the need for a binding contract between the controller and processor with its various contractual stipulations (see above), additional requirements imposed on processors will include the following.

- Processors must not engage sub-processors without the controller's prior specific or general written authorisation, including changes to sub-processors after general written authorisation has been given – so giving the controller the opportunity to object to those changes: article 28(2). This could clearly have a material impact on cloud supply chains and changes to them. Moreover, where a processor has engaged sub-processors, it must impose by contract the same data protection requirements on those sub-processors as apply in the controller-processor 'head' contract, in particular to ensure that sub-processors provide sufficient 'guarantees' to implement appropriate technical and organisational measures to meet the requirements of the GDPR. Processors will be liable to controllers for the acts and omissions of sub-processors (article 28(4)).
- Processors must keep a written or electronic record of all categories of processing activities undertaken for a controller (article 30(2)). There is an exemption for organisations employing fewer than 250 employees, with certain exceptions (article 30(5)).
- There is a specific requirement for processors to cooperate with data protection supervisory authorities (article 31).
- Another new set of obligations on processors relates to data security and breach reporting. In their own right, processors must – having regard to the state of the art, costs, risk, etc – implement appropriate technical and organisational measures to ensure data security, including the pseudonymisation and encryption of personal data; the confidentiality, integrity, availability and resilience of processing systems and services; the restoration and availability of data following 'physical or technical' incidents; and regular security testing (article 32(1)). The economics of cloud computing – especially in public cloud deployment models – are likely to be challenged by these requirements.
- Under article 33(2), the processor must notify the controller 'without undue delay' after becoming aware of a personal data breach. This must be seen in the context of the controller's new obligation to notify its supervisory authority – except for breaches unlikely to compromise data subjects' rights – without undue delay and, where feasible, not later than 72 hours after becoming aware of a data breach, including details surrounding the breach (article 33(1) and (3)). CSP processors are often therefore required to support B2B customer controllers in breach management and notification, which will in turn need to be reflected in cloud arrangements and contracts.

Sanctions and remedies

Under the GDPR controllers and (as mentioned above) processors will be directly accountable and liable for non-compliance, both to data subjects and regulators. The allocation of responsibility and liability for infringements as between cloud customers and CSPs has, therefore, assumed even greater importance in B2B and B2C-related cloud contracts – particularly because of the extent and scale of the GDPR sanctions and remedies.

Any person who has suffered 'material or non-material' damage as a result of an infringement will have a right to receive compensation from the controller or processor (article 82(1)). Controllers will remain liable overall for such damage, while processors will only be liable where they have not complied with the GDPR obligations specifically directed to them or where they have acted outside or contrary to the lawful instructions of controllers (article 82(2)).

Administrative fines will depend on the gravity of the non-compliance (article 83(2) (a)–(k), 83(3)). There are two tiers of fine for specified infringements: a lower level of up to €10 million or, in the case of businesses, up to 2 per cent of the preceding financial year's worldwide annual turnover, whichever is higher (article 83(4)); and an upper level of up to €20 million or, in the case of businesses, up to 4 per cent of the preceding financial year's worldwide annual turnover, whichever is higher (article 83(5)).

There are other processes and sanctions available for non-compliance under both the GDPR and the DPA, including audits, access rights, reprimands and administrative orders (article 58).

Cross-border data transfers

These rules are dealt with in articles 44 to 50. As applied to cloud computing and cloud supply chains, they are an important part of the GDPR's regulation. Personal data transfers to recipients in 'third countries' continue to be closely regulated, broadly to ensure that the level of data protection for data subjects is not undermined (article 44). Overall, the GDPR framework for such transfers is similar to that under the previous Data Protection Act 1998 and Data Protection Directive, with some useful new compliance measures, including the ability of data exporters to demonstrate compliance through approved codes of conduct and approved certification mechanisms (article 46(2)). Breach of these provisions will be a non-compliance issue for which the upper tier of administrative fines can be imposed (see sanctions and remedies above). Both controllers and processors will be liable to non-compliance proceedings.

Uncertainty looms over the adequacy of the SCCs (also known as model clauses) approved by the European Commission as a means of ensuring adequate protection of personal data when transferred to recipients in third countries. The *Schrems II* litigation (*Facebook Ireland*

& Schrems (Case C-311/18)) (*Schrems II)*, the opening arguments of which were heard in July 2019, concerns whether these clauses provide a sufficient degree of protection for personal data transferred to the US. The SCCs are the most widely used international transfer mechanisms for personal data, meaning that a ruling by the Court of Justice of the European Union (CJEU) invalidating the clauses would have a wide-ranging impact on businesses. The CJEU's judgment is expected to be handed down in early 2020.

Privacy Shield

Adopted by the European Commission in July 2016 (http://europa.eu/rapid/press-release_IP-16-2461_en.htm), this applies to EU–US data transfers and is relevant for cloud computing in EU–US and related trade. Microsoft claimed to be the first US CSP to appear on the US Department of Commerce's list of Privacy Shield certified entities (https://azure.microsoft.com/en-gb/blog/microsoft-cloud-is-first-csp-behind-the-privacy-shield/). At the time of writing, the Privacy Shield is also under threat, as the European Parliament has issued a resolution requesting that the European Commission suspend the Privacy Shield until such time as the USA can demonstrate full compliance with its terms and this mechanism is also susceptible as a result of the *Schrems II* litigation referred to above.

Access to EU personal data by third country governments

In the light of the Snowden disclosures and the litigation that followed them (eg, *Microsoft v United States*, No. 14-2985 (2d Cir. 2016) http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html), it is worth noting that article 48 of the GDPR contains specific safeguards against third country governments' access to EU personal data. Any third country judgment or administrative decision requiring a controller or processor to disclose EU personal data will only be enforceable if it is based on an international agreement, for example a mutual assistance treaty between that third country and the EU or a member state. (See also question 10 on MLAs; and the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003 at http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461&back=5441.)

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)?

It follows from the answer to question 1 that, in the UK, contracts cover the full range of cloud service and deployment models and reflect the UK's large and sophisticated cloud business ecosystem, including CSP supply chains.

One aspect of cloud contracting that tends to cause difficulties for cloud customers is where, as is typical, cloud contract formats are modular. This means that the provisions of the contract must be located from a combination of offline and online sets of terms or – more typically – from a combination of multiple online sets of terms, policies, etc, which users must access by clicking on different hypertext links. These sets of terms are then assembled and stipulated by the CSP to form the entire contract. In my experience, these formats and contract processes make it difficult even for sophisticated corporate customers to ascertain the full extent of cloud contracts and, in some cases, to determine what terms will govern them. In B2C contracts, and possibly where B2B cloud customers are negotiating on CSP standard terms of business, this difficulty in ascertaining applicable contractual terms could in certain circumstances ultimately result in the legal ineffectiveness or unenforceability of certain contract terms and lead to regulatory intervention.

The answers to questions 17 to 22 are based on a review and knowledge of a limited, but meaningful, range of B2B public cloud service agreements (CSAs) and related documents proposed by the major international CSPs that are available from public resources. It is beyond the scope of this work to survey a much wider range of such contracts or to segment them by deployment model, service model or specific cloud services within each service model. (Readers are referred to the work of leading UK academics, including *Cloud Computing Law*, Christopher Millard (ed), (Oxford University Press 2013), noting that, inevitably there will have been changes to CSA practice and terms since. I also wish to acknowledge the excellent reports and other deliverables produced by the (now decommissioned) SLALOM Project teams, which I used to sense-check my own review of the CSAs referred to above. SLALOM documentation is recommended reading for this area and may be downloaded from the links at: https://cordis.europa.eu/news/rcn/134076_en.html, using 'slalom' as a search term.

The answers below do not identify CSPs by name;: they reflect a composite, high-level, view of the CSAs and related materials reviewed. Moreover, they do not attempt to assess the reasonableness, fairness or validity of the terms outlined. Here, I adopt the approach taken by the SLALOM Project team: readers will be aware that, in assessing these matters, much will depend on the context of the service and deployment and service model or models adopted, the relative bargaining strength of the parties, the economic basis of the cloud arrangement, cost or no-cost, and whether it is a beta product or service, etc.

The European Commission actively promotes the development and use of fair standard cloud computing contracts and there will be further developments under this initiative (see https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-service-level-agreements).

Finally, the role of international standards will be ever more important as applied to cloud computing services, service level agreements (SLAs) and CSAs (see for cloud computing and distributed platforms ISO/IEC JTC1 SC38, https://www.iso.org/committee/601355.html).

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?

With limited exceptions, the governing law of the CSP's home jurisdiction or a chosen regional location will apply. For certain purposes, for example, EU data protection SCCs, the choice of governing law and jurisdiction may be those of the customer's location. Courts (rather than arbitral tribunals) competent in the CSP's jurisdiction are most commonly chosen. US CSPs usually require all customers to commit to compliance with applicable US export controls, sanctions and related laws and regulations.

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?

Pricing and payment

Pricing will, of course, vary depending on the deployment and service model offered, and whether the contract is formed on- or offline. Some

CSPs reserve the right to vary charges for existing services. There are usually remedies for late payment, including interest and, in some cases, the right for the CSP to suspend service for payment defaults. If the customer defaults on payment when due, all CSAs reviewed entitle the CSP to terminate them (see question 22).

Suspension of service by the CSP

It is common to see suspension rights in addition to specific termination rights (and sometimes for the same or overlapping triggering events). The most typical cause for suspension is where there has been a breach by the customer or an end user of the acceptable use policy (AUP – see below), which will usually include the customer or an end user causing security risks to the cloud service, the CSP or other cloud service users, or infringing third-party rights. Suspension may be on notice or, where urgent (as in the case of security risks), without notice. In some cases, the customer will remain liable to pay the charges during the suspension period, while service credits (see below) will not accrue.

Acceptable use policy

The CSAs of all the major CSPs contain an AUP: it has become one of the defining features of CSAs in the UK as elsewhere. Readers will be familiar with the standard terms of AUPs, which address conduct by both customers and their end users in using the cloud services, and will include prohibitions on:

- illegal activities of any kind;
- violation of any third-party rights;
- gaining or attempting to gain unauthorised access to any networks, systems, devices or data;
- unauthorised disruption of any networks, systems, devices or data;
- sending unsolicited messages or marketing; and
- distributing malware.

As stated above and under question 22, breach of the AUP may entitle the CSP to suspend or terminate the CSA – in some cases, the breach of a single end user could result in suspension or termination. Other CSAs contain indemnities for AUP breaches. Where the AUP has been breached, or the CSP suspects it has been breached by illegal conduct, the CSP may report those activities to the authorities or interested third parties and reserve the right to cooperate with them.

Variation

One of the more disquieting terms of CSAs in the UK as elsewhere is that CSPs may without the customer's consent vary cloud services, SLAs and other terms of the CSA – usually without any justification and in some cases even without the obligation to notify customers beforehand. Typically, when exercised, variation does not entitle the customer to terminate the CSA.

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?

To reflect the entry into force of the GDPR, all the major CSPs operating within, or providing services to, the EEA introduced detailed data protection and processing terms for incorporation into their CSAs, in some cases in separate addenda or supplements.

Typically, the GDPR-related terms include:

- the allocation of processor and controller roles and functions between the customer and the CSP, with the CSP as processor and with the right for the CSP to appoint sub-processors (subject to the customer's right to object to the appointment of new sub-processors and with concomitant sub-processor obligations);
- the application of technical and security features provided to the customer to enable it to comply with the technical and organisational measures required by the GDPR;
- deeming of 'documented' customer instructions to the CSP with regard to the CSP's processing of customer data in accordance with the GDPR;
- confidentiality obligations of the CSP in relation to customer data;
- terms for the handling of data subject access requests;
- detailed operational security provisions, including security breach notification obligations on the CSP;
- CSP data security certification and audits;
- provision for the transfer of personal data outside the EEA, with the incorporation of the SCCs accordingly;
- the return or deletion of customer data on termination of the CSA;
- obligations relating to record keeping of all processing activities; and
- terms ensuring the processor's cooperation with the relevant regulator in the performance of their duties.

As at the time of writing, there have been no reported legal challenges emanating from the UK to CSP GDPR terms.

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?

Liability

Understandably, all CSAs contain limitations and exclusions of liability: some are written from a US perspective, while others are localised. The CSP's liability is commonly limited (sometimes mutually) to the amount of charges paid by the customer – usually during the 12 months preceding the event giving rise to liability. Liability caps of this kind are sometimes tiered by reference to different services, for example the greater of a specified monetary amount or the total charges paid, depending on the service.

Some CSAs exclude from this limitation the CSP's liability for third-party IPR infringements (whether under an indemnity or otherwise), and for confidentiality and data protection breaches.

It is common for CSAs to exclude liability:

- in general for indirect, consequential, incidental, exemplary, punitive or special losses or damages (even if some of those kinds of loss or damages are not recognised in the UK jurisdictions); and
- for a range of specific losses, including loss of revenue, loss of profits, loss of customers or goodwill, loss of use of data, loss of anticipated savings, loss of the use of the cloud service, etc.

Some CSAs disclaim liability for unauthorised access to, and for loss or destruction of, uploaded content and data. In other cases, CSAs will acknowledge the CSP's liability for content or data loss where the CSP has failed to meet its own security obligations. Many CSAs require customers to take responsibility for making backup copies of their own content and data or otherwise mitigating their own risks in using the cloud service.

Warranties and provision of service

Some CSAs contain a CSP warranty that it will deliver the services in accordance with the SLA or some other service description. Some CSAs state that cloud services are provided 'as is'. Almost invariably, any other express or implied warranties (eg, as to fitness for purpose, satisfactory quality, non-infringement) are disclaimed to the extent permitted by law. Some CSPs specifically exclude any express or implied warranty that the operation of the cloud service or software made available through it will be uninterrupted or error-free.

Also, typical of many CSAs is that customers will not be entitled to claim for service unavailability for scheduled or unscheduled downtime or other service interruptions.

Indemnities

It is common for the customer to have to indemnify the CSP against the customer's and any end user's:

- act or omission or use of the cloud service that infringes any third party's rights;
- breaches of the CSA generally and the AUP specifically;
- infringement of applicable law;
- creation or use of uploaded content; and
- in each case where the act, omission, use, etc, gives rise to claims, costs, losses, and so on.

Where there are detailed data processing provisions, including data transfer agreements (see question 19), some CSAs will provide for customer indemnification of the CSP against breach of data protection law caused by the customer or an end user.

For the CSPs' obligations to indemnify or (quite commonly) to defend the customer against third-party IPR infringement claims or final judgments, see question 21.

Service availability, quality, service levels and service credits

Many B2B public cloud CSAs contain or incorporate by reference specific SLAs as applicable to the service modules provided to the customer. (For an example of CSA service levels applied by the major CSPs (and some others), readers are referred to the SLALOM Project's documentation available from the links at: https://cordis.europa.eu/news/rcn/134076_en.html, using 'slalom' as a search term.

The application of specified service credits is usually expressed to be the sole and exclusive remedy for service-level breaches. Some CSPs make specific claims or promises about their levels of service and are willing to enable the customer to terminate the CSA for stipulated breaches of those service levels, subject to following mandated procedures for doing so, with repayment of any prepaid charges. Many CSAs contain caps on the maximum amount of service credits allowable in a specified period.

Commonly, CSAs do not provide specific SLA breach reporting mechanisms, which would of course make monitoring and enforcing the SLA or service credit regime difficult for the customer. In other situations, customers are required, within stipulated deadlines, to follow specified procedures to report the service level breaches, as well as providing details of them for verification by the CSP, who may retain the option of rejecting the customer's claim.

Some CSAs entitle the CSP unilaterally to vary the SLAs and service credits.

It is usual for CSAs to exclude the operation of the SLA, where for example:

- there is a force majeure event;
- the customer or an end user is in breach of the AUP or other terms of the CSA;
- the services have been lawfully suspended;
- the service outage is attributable to technology not provided by the CSP; and
- the CSP's systems are down for maintenance.

See also question 20 under 'Warranties'.

Business continuity and disaster recovery

In general, unless the CSP is providing a cloud-based business continuity service, CSAs do not contain any, or in any detail, business continuity or disaster recovery terms – although it is typical for CSAs to contain force majeure provisions excusing the CSP's performance in such cases. This is a feature of CSAs in the UK, US and elsewhere (see the useful report, Public Cloud Service Agreements: What to Expect and What to Negotiate Version 2.0 produced by the US Cloud Standards Customer Council, www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf, which may at the time of publication have been updated and available online).

Usually, the customer is expected or obliged to make its own backup arrangements to ensure continuity. Sometimes, CSAs will refer to CSPs having their own disaster contingency plans for their data centres, using redundant processing and storage capacity to back up data held in those data centres, but without any contractually binding commitment to implement such plans.

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?

Typical terms are as follows.

- The customer usually warrants that it owns or has all necessary rights to use its content (eg, software, data) processed by the cloud service or to grant any licences to the CSP under the CSA, and that its content or end users' use of the customer's content will not breach the AUP (which may entitle the CSP to suspend or terminate the CSA).
- The customer retains IPR in the contents uploaded or created by it in using the cloud service. The CSP may use the contents to provide the cloud service or to comply with regulatory or governmental directions or orders.
- The CSP may use without restriction any suggestions for improvements to the cloud service made by the customer, in some cases, with an obligation to assign ownership in such suggestions to the CSP.
- The CSP reserves rights in all IPR relating to its cloud services, including IPR in the applications and infrastructure used in providing the services.
- If the cloud services are found, or understood by the CSP, to infringe any third-party IPR, the CSP may at its discretion, and usually as a preferred remedy, procure the necessary rights for customers to continue using the services, modify the services so that they become non-infringing without any material loss of functionality, or provide equivalent services in substitution for the infringing services – or failing that, to terminate the cloud services concerned. In some cases, instead of the above 'work around' language, the CSP will undertake to defend or indemnify the customer against the claims, costs, losses, etc, arising from final judgments. Where CSAs are governed by the laws of a US jurisdiction, customers may find that the obligation to defend does not include the obligation to indemnify – though this is, of course, to be determined under the relevant US jurisdiction if validly chosen.

Typical terms covering termination

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

CSAs may allow termination for convenience on specified notice for both the customer and the CSP.

Either party will usually have a right to terminate for the (unremedied) material breach of the other, change of control of the other, or

the insolvency of the other. There is often also a range of specific rights of termination by the CSP, including:

- non-payment by the customer of due invoices;
- where the cloud service is dependent on third-party IPR (eg, software) licences, when a relevant third-party licence expires or is terminated;
- for a specified period of customer inactivity;
- where the customer or an end user's use of the cloud service presents a security risk to the CSP or any third party (typically contained in the AUP);
- contravention of export and sanctions controls laws and regulations; and
- one or more (other) breaches of the AUP or any other term of the CSA by the customer or an end user.

The consequences of termination may include:

- the customer's obligation to cease using or to return any proprietary material (eg, software), or to destroy any content provided by the CSP;
- that the CSP will not erase the customer's data for a specified period after termination, and in some cases that the customer will be entitled to retrieve its data (usually also subject to a charge by the CSP);
- where the CSP has terminated for cause, that the customer must pay all unpaid charges for the remainder of the term; and
- where the customer has terminated for cause, that the CSP will refund any prepaid charges for the remainder of the term.

Employment law considerations

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

There are none that apply specifically to cloud computing.

However, depending on the cloud deployment model or service model adopted and the circumstances of the migration to cloud or the termination of the cloud service, cloud customers and CSPs should consider the application of the Transfer of Undertakings (Protection of Employment) Regulations 2006 (www.legislation.gov.uk/uksi/2006/246/contents/made), as amended by (among others) the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 (www.legislation.gov.uk/uksi/2014/16/regulation/1/made#regulation-1-2) (together, TUPE). TUPE implements in the UK the EU Acquired Rights Directive 2001/23/EC (ARD).

The application of the ARD and TUPE to, and their effect on, outsourcing are now widely understood in relation to the UK, where the government has expanded TUPE's application to outsourced services with the intention that TUPE should generally apply to outsourcing transactions. It is worth reiterating that TUPE is mandatory law: parties cannot 'disapply' or contract out of TUPE.

In broad terms, where TUPE does apply, it transfers automatically by operation of law the staff from one organisation to another. Their terms and conditions of employment and continuity of service are preserved, and there are other procedural and substantive protections for the staff before and after a 'TUPE transfer', for example protection against dismissal and protection against changes to the transferring staff's terms and conditions of employment. There are also prescribed consultation processes before any transfer (see generally www.acas.org.uk/index.aspx?articleid=1655). Accordingly, if TUPE applies to a cloud computing arrangement (in which one of the key drivers is cost-reduction) the financial implications for both the cloud customer and more particularly the CSP may be significant and could undermine the economics of the arrangement.

In the UK, the most relevant trigger for TUPE in the context of cloud computing will be where an in-house IT service ceases to be provided by the customer itself and is then provided by the CSP – or is migrated to another CSP after the initial cloud migration, or back to the original customer, if it wishes to resume the IT service in-house. This can constitute a service provision change under TUPE Regulation 3(1)(b). The workforce (organised grouping) carrying on the activities liable to transfer must be based in Great Britain and the principal purpose of that workforce must be to carry out those activities for the customer. In broad terms this means they must be 'essentially dedicated' to the customer; although they may still do work for others (TUPE Regulation 3(3); and see generally www.gov.uk/transfers-takeovers). More significantly for cloud computing arrangements, the activities to be carried out by the CSP must be 'fundamentally the same' as those undertaken previously by the customer's staff (TUPE Regulation 3(2A) www.legislation.gov.uk/uksi/2014/16/regulation/1/made#regulation-1-2).

So, the threshold question in cloud computing migration is most likely to be: will the activities to be undertaken by the CSP be 'fundamentally the same' as those undertaken previously by the customer's IT staff? This will come down to an analysis of fact and degree. One – and only one – factor will be a reduction in the volume or scope of work, which is likely to be the case in migration from 'traditional' IT activities to the cloud (see *Department for Education v Huke and another* UKEAT/0080/12, https://www.bailii.org/uk/cases/UKEAT/2012/0080_12_1710.html; *OCS Group UK Ltd v Jones and another* https://www.bailii.org/uk/cases/UKEAT/2009/0038_09_0408.html).

At first glance, IT activities or services migrated to, say, a public or hybrid cloud, from which the customer may then receive very different cloud services (at least by reference to scope and possibly volume) to the services or activities previously provided in-house, simply do not intuitively look and feel 'fundamentally the same' in the cloud. And – if they addressed the question at all – it would be understandable if the customer and CSP considered that the activities to be carried out by the CSP are not 'fundamentally the same' as the original in-house IT activities, so that TUPE would not apply. This could be a very costly mistake.

There will, of course, be other questions about which of the customer's staff members and how many of its IT workforce are in scope for TUPE, if it is likely to apply (see www.gov.uk/transfers-takeovers).

And it is worth reiterating that TUPE can apply equally to the subsequent move by the customer from one CSP to another, or back in-house to the customer, subject to the rules referred to above.

In cloud computing arrangements, it is quite likely that the CSP will be based outside the UK or that the cloud services will be provided from an offshore location. If there is an assigned workforce based in Great Britain, TUPE can apply to such arrangements, even if the service is provided from offshore.

In outsourcing transactions, because the application of TUPE is so well settled in the UK, it has become customary for the customer and outsource provider to provide specifically and in some detail in the outsourcing contract for the legal, regulatory and financial implications of TUPE – allocating duties, risk, costs and liabilities between them. In public and hybrid cloud contracts, the issue is often simply not considered and, therefore, is not provided for, most probably because the parties do not expect that TUPE will apply to such cloud arrangements or because CSPs that are based outside the EU are unaware of the ARD and TUPE.

For the reasons given above, neither CSPs nor their customers should assume that TUPE cannot or does not apply in relation to any of the cloud deployment models or service models. They should at least consider the question and take advice accordingly.

TAXATION

Applicable tax rules

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

Consideration of the tax treatment of cloud computing will generally be more complex than in the case of 'terrestrial', in-country-only, IT services. This is because tax authorities and businesses alike are grappling with the tax implications of cloud computing. The first step required is to correctly classify the underlying transaction in order to ascertain the correct tax treatment. Individual elements within the scope of, and transactions comprising, the cloud services will need to be analysed, in order to determine whether there is a transfer of property to the customer (ie, a sale, lease or licence of tangible property). If there is no such transfer then it is necessary to consider the tax rules in respect of the provision of services, assuming that the cloud services are properly characterised as services (eg, data processing, an information service or a communications service). Consideration will also need to be given to the location of the CSP and its customers, to the source of the payments, and also to whether the location of the servers from which the services are provided can give rise to taxation.

The approach to taxation will also depend on the operating model of the supply chain of the cloud service, for example whether it is intra-group or there are external providers in the supply chain and, if intra-group, whether the local CSP subsidiary performs sales and marketing functions for another group company or delivers the cloud services directly to local customers. (For an invaluable guide see Ernst & Young's Worldwide Digital Tax Guide, www.ey.com/gl/en/services/tax/ey-digital-tax-guide.)

The following is a high-level outline of the UK taxes that are likely to be most relevant to cloud computing operations and the income derived from them. Readers – both CSPs and cloud customers – should seek specific advice on direct tax questions relating to UK cloud operations and service arrangements. And for tax and other fiscal incentives available for cloud computing businesses in the UK, see questions 6 and 7.

Corporation tax and permanent establishment (PE)

A company resident in the UK is subject to tax on the whole of its worldwide profits wherever they arise. A non-resident company is liable to corporation tax on profits attributable to a trade carried on in the UK through a PE in the UK. In determining whether a PE exists, the UK broadly adopts the OECD definition of PE. If a non-UK resident CSP has a fixed place of business in the UK through which some or all of its business is conducted, or has an agent acting on its behalf, it may be treated as having a PE in the UK and may be liable to UK corporation tax (currently 19 per cent but reducing to 17 per cent in April 2020). Will the presence of cloud servers in the UK be decisive in the determination of a PE? The HM Revenue & Customs (HMRC) approach is that the mere presence of a server or servers will not of itself create a PE. However, if the CSP is providing hosting services and the UK servers are essential for that hosting, this may result in the existence of a PE. Ultimately, whether a server will create a PE will depend on the functionality of the server or servers as well as the business activities in the UK.

UK diverted profits tax

Introduced in the Finance Act 2015 to counter the use of aggressive tax planning techniques by multinational enterprises to divert profits from the UK, this tax is also known as the 'Google tax'. It is charged at 25 per cent when a foreign company artificially avoids having a UK taxable PE or when a UK company, or a foreign company with a UK PE, would benefit from a tax advantage (ie, a reduced UK tax liability) through the use of group structures, entities or transactions that lack economic substance. HMRC will consider various aspects of the structure, including the allocation of profits throughout the supply chain. (See generally www.gov.uk/government/publications/diverted-profits-tax-guidance.) Certain amendments were introduced in the Finance Act 2019, which took effect from 29 October 2018 (see https://www.gov.uk/government/publications/diverted-profits-tax-changes/diverted-profits-tax-amendments) .

Withholding taxes

Withholding taxes may apply at the rate of 20 per cent to sales, services and (in broad terms) income derived from annual payments, patent royalties and certain other payments arising from the exercise of intellectual property rights paid by a UK resident company to a non-UK resident person who is not a corporate taxpayer, subject to reduction under an applicable tax treaty. For example, withholding taxes may apply where in a CSP group structure, a non-UK, IPR-owning or licensor group company has put in place intra-group IPR licensing arrangements and the UK-based group CSP is required to remit payments to the non-UK licensor for the exploitation, licensing or distribution of that IPR. New legislation was enacted in the UK in 2016 to address the abuse of double taxation treaties in this context. (See, generally, http://taxsummaries.pwc.com/ID/United-Kingdom-Corporate-Withholding-taxes.)

Offshore Receipts in respect of Intangible Property

Following a consultation, the UK government has introduced a new income tax charge on offshore receipts from intangible property (ORIP). From 6 April 2019, non-UK residents in certain (generally low-tax) jurisdictions will be liable to UK income tax on their gross receipts from intangibles to the extent the IP enables, facilitates or promotes UK sales. The aim is to ensure that businesses generating income from UK sales are not able to artificially achieve low effective tax rates by holding their IP offshore (see: https://www.gov.uk/government/publications/offshore-receipts-from-intangible-property/income-tax-offshore-receipts-in-respect-of-intangible-property). ORIP applies only if UK sales by the non-UK resident (and its connected persons) for a given tax year exceed £10m, but it applies whether or not the non-UK resident has any presence in the UK. There are several exemptions that are currently available and the government has proposed additional exemptions in draft regulations released recently.

It is expected that the final regulations will be made available in Autumn 2019 and that parts of the regulations will have retrospective effect (see https://www.gov.uk/government/consultations/draft-regulations-offshore-receipts-in-respect-of-intangible-property). Businesses will need to determine whether their IP enables, facilitates or promotes UK sales, either directly or indirectly, and even through unrelated parties. Taxpayers may find it difficult to trace through often complex supply chains to determine whether their IP is supporting UK sales.

Taxing the digital economy

The UK government has announced that it will introduce a new Digital Services Tax in April 2020. This will be introduced as an interim measure, until a multilateral solution that is acceptable to the UK is adopted. The UK government has stated that it intends to disapply the tax once an appropriate international solution is in place. The UK has focused on 'user participation'. The government views user participation as being a key value driver for digital businesses and the legislation will target digital business models, where value is actually created as a result of the active participation and engagement of UK users of digital platforms. The business models that may be impacted by these proposals include online networks, social media platforms and search engines. To the extent that these models are served by cloud computing services and CSPs, they are likely to be relevant to the cloud computing industry operating in, or targeting customers in, the UK.

The digital services tax legislation will be introduced in the Finance Bill 2019-20 and will apply to revenue earned from 1 April 2020. Businesses will become liable to the tax when the group's worldwide revenues from in scope digital activities are more than £500 million and more than £25 million of these revenues are derived from UK users. If the group's revenues exceed these thresholds, its revenues derived from UK users will be taxed at a rate of 2 per cent. The first £25 million of the UK revenues would be exempt from the digital services tax (see https://www.gov.uk/government/publications/introduction-of-the-new-digital-services-tax/introduction-of-the-new-digital-services-tax). These thresholds mean that only the very largest multinationals will be caught, so while CSPs may be involved with in-scope activities, the thresholds may exclude them in practice.

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.

Again, readers – both CSPs and cloud customers – are advised to seek specific advice on indirect tax questions relating to UK cloud operations and service arrangements.

The rules for applying value added tax (VAT) to electronically supplied services differ depending on whether the CSP and its customers are inside or outside the UK or the EU; whether the cloud services are for business or personal use; and if they are B2B supplies, whether they are 'used and enjoyed' within the UK, elsewhere in the EU or outside it.

A UK CSP will be expected to register and be liable to charge and account for VAT on the supply of cloud services delivered in the UK. However, specific consideration should be given to CSP intra-group arrangements, particularly the structure of, and transactions under, those arrangements. Non-UK principals are not expected to be VAT-registered. For B2B cloud transactions supplied in the UK by a UK CSP VAT at the standard rate of 20 per cent will generally be payable in respect of cloud services. Cloud customers will be expected to account themselves for VAT on payments for services provided by non-UK based CSPs – the cloud customer should act as if it is both the supplier and the customer: it charges itself the VAT and then, assuming that the service relates to VAT taxable supplies that it makes, it can claim the VAT back (so rendering the transaction VAT-neutral). In terms of the CSP, the service is disregarded, and it does not need to account for any VAT. This is called the 'reverse charge', but is also known as a 'tax shift'.

For B2C cloud transactions VAT at the standard rate of 20 per cent will generally be payable. A UK CSP will usually be registered and liable to charge and account for VAT on the supply of cloud services in the UK.

Non-UK CSPs providing cloud services to UK consumers should particularly note that the VAT rules for digital services (eg, webhosting services, internet-streaming services, database storage, supplies of software and software update services, and other electronically supplied services) do not follow the standard place of supply rules. The services are treated as supplied in the 'place of residence of the consumer' (and not the place of residence of the supplier). VAT is, therefore, payable, on, and CSPs are VAT-accountable for, supplies of digital services to UK consumers, regardless of whether the CSPs are established in or outside the EU (www.gov.uk/government/publications/vat-supplying-digital-services-to-private-consumers/vat-businesses-supplying-digital-services-to-private-consumers). Accordingly, a CSP established and operating outside the EU that sells digital services to UK consumers (and consumers in other EU member states) will be required either to register for VAT in each EU member state where it has customers and comply with all local VAT rules, or to register for the EU's VAT Mini One Stop Shop (MOSS) scheme in a single EU member state (which should rationalise the VAT accounting requirements).

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.

Pippa Middleton and James Matthews v Person or persons unknown [2016] EWHC 2354 (QB)

The iCloud account of the sister of the Duchess of Cambridge had been hacked, apparently resulting in the theft of some 3,000 images. Ms Middleton and her then fiancé, Mr Matthews, had successfully applied for an interim privacy injunction against persons unknown to prevent the use, publication or disclosure of the stolen images. In this case, they successfully applied for a continuation of the injunction and the extension of its scope to cover material and information from the iCloud account other than images, because Ms Middleton had good reason to believe that all the information in her iCloud account had been hacked, not just her photographs. As reliance on iCloud and similar B2C storage services grows even more widely, such cases are likely to become more frequent, especially where prominent personalities are involved.

Skyscape Cloud Services Ltd v Sky Plc [2016] EWHC 1340 (IPEC)

Skyscape supplied cloud services to UK public sector organisations under the G-Cloud scheme (see question 1). Sky Plc is a well-known UK provider of broadcast and communications services (including an email service) under the trademark 'SKY'. Sky Plc claimed trademark infringement against Skyscape, the CSP, which sought a declaration of non-infringement (DNI) for its marks 'SKYSCAPE' and 'SKYSCAPE CLOUD SERVICES' as applied to its cloud services. The court found that there was a likelihood that a significant part of the relevant public and therefore the average consumer, seeing the sign SKYSCAPE used for an email service, would confuse it with yet another service offered by Sky Plc. The DNI was refused. This case is mentioned because of the apparent popularity of the word 'sky' in the branding of cloud services and the position of Sky Plc in the UK market, together with its registered SKY trademarks. In the result, Skyscape was rebranded as UKCloud (see question 3, and for the background: www.theregister.co.uk/2016/07/28/skyscape_now_uk_cloud/). Unless CSPs are willing to forgo the use of 'sky' in branding and marketing their cloud services in the UK, cases of this kind will proliferate (see *Sky Plc and others v SkyKick UK Ltd and another* [2018] EWHC 155 (Ch) http://www.bailii.org/ew/cases/EWHC/Ch/2018/155.html; and also *British Sky Broadcasting Group plc and others v Microsoft Corporation and another* [2013] EWHC 1826 (Ch) below). Similar disputes have arisen about the use of the word 'cloud'. For example, in *Massive Bionics v EUIPO*, www.bailii.org/eu/cases/EUECJ/2017/T22316.html, the EU General Court partially upheld an opposition by Apple to the registration of 'Dricloud' for cloud services by Massive Bionics on the basis that this sign was similar overall to Apple's own trademark 'iCloud' also covering cloud services.

Majekodunmi v City Facilities Management UK Ltd and others [2015] UKEAT 0157_15_2509

In this case, the UK Employment Appeal Tribunal (EAT) had to consider whether the claimant had validly served his notice of appeal when the attachments containing his notice could only be accessed by a link to Dropbox, the cloud-based file-hosting service. The EAT rejected the claimant's case, finding that sending a link to where a required document is located online is not 'serving' or 'attaching' that document. Although zip files are a valid form of service, in this case the EAT needed the internet to access the zip file location in the cloud. The file had,

therefore, not 'hit' the EAT's server as a standard attachment to an email would. The EAT then had to decide whether the documents were effectively 'attached' to the email purporting to serve the required notice. It held that they were not, because all that had been provided was a link to another location where the documents could be found – the documents themselves had not actually been attached. This is a significant decision for users of cloud-based file-hosting services such as Dropbox. The case also contains an interesting legal consideration of the cloud storage and transmission technologies used. It will be worth watching the development of court and tribunal rules in this regard.

British Sky Broadcasting Group plc and others v Microsoft Corporation and another [2013] EWHC 1826 (Ch)

The court ruled that Microsoft's 'SkyDrive' mark for cloud storage services infringed British Sky Broadcasting's 'SKY' UK and (EU) Community trademarks. The court's decision was influenced by the fact that consumers were unable to discern any Microsoft connection to SkyDrive as a preloaded app on any device. This finding was supported by evidence that 17 British Sky Broadcasting (Sky) customers had contacted Sky's helpline, because they assumed (in actual confusion) that SkyDrive was a Sky-provided service.

Microsoft contested the validity of Sky's UK SKY trademarks in their application to 'goods and services pertaining to cloud storage'. It alleged that:

> *'sky' is a convenient and common word used by traders to describe or allude to a cloud storage system (be that system a good or a service) such that (a) it is incapable of distinguishing a cloud storage system of one undertaking from that of another, and (b) it should be kept free for use by all traders offering such systems.*

Microsoft also claimed that the word 'sky' would be 'recognized by the average consumer as descriptive of a characteristic of a cloud storage system, namely by indicating that the system is for the storage of data remotely, being notionally in 'the cloud' or 'the sky''. Microsoft's challenge of invalidity was rejected.

Aside from the linguistic and symbolic connections between 'sky' and 'the cloud', the case is also interesting because of the judge's technological comparison between broadband services and certain cloud services. He said:

> *It seems to me that the evidence reveals that there is a close connection between file storage, management and sharing software and the provision of broadband services, including the provision of email services . . . Not all data storage providers are broadband providers but it seems to me that the evidence reveals that a significant number of broadband providers also provide data storage.*

In 2014, Microsoft rebranded 'SkyDrive' as 'OneDrive' (www.techrepublic.com/article/microsoft-renames-skydrive-to-more-confusing-onedrive-amid-legal-complaint/).

BRYAN CAVE LEIGHTON PAISNER BCLP

Mark Lewis
mark.lewis@bclplaw.com

Adelaide House
London Bridge
London EC4R 9HA
United Kingdom
Tel: +44 203 400 1000
Fax: +44 203 400 1111
www.bclplaw.com

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?

None.

* *The author would like to thank BCLP colleagues Faiza Bishi, Kate Brimsted, Sarah Buxton, Gillian Dennis, Daren Kemp, Sophie Taylor, Adam Turner and Ash von Schwan for their assistance in writing this chapter.*

United States

Amy Farris, Manita Rawat and Matthew Mousley*
Duane Morris

MARKET OVERVIEW

Kinds of transaction

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

All manner of cloud computing transactions take place in the United States, including public, hybrid and private cloud models and software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) models. There is a growing trend in both the private and public sectors to utilise cloud offerings not only for the benefits of such offerings over legacy models, but out of necessity, as a growing number of products and services procured by businesses and governmental entities are being replaced by cloud-only offerings.

The most common examples of public cloud offerings are service providers who provide software applications (ie, SaaS) and data storage to the general public. By comparison, the most popular private cloud offerings are IaaS, which permits a customer to access IT infrastructure services as a service, and PaaS, which can include a variety of services from simple cloud-based applications to more sophisticated enterprise applications. As noted above, because cloud offerings have begun largely to replace legacy offerings, in practice, most customers implement and integrate public and private cloud offerings to create a hybrid cloud environment.

In addition to the considerable cloud offerings available to the private sector in the US, there are a number of notable government platforms for cloud computing, including Amazon Web Services (AWS) GovCloud and Microsoft Azure Government. These platforms address the specific regulatory and compliance requirements required by government agencies and customers, including adherence to the US International Traffic in Arms Regulations requirements. See:

- http://fortune.com/2016/09/02/us-government-embraces-cloud/;
- www.wired.com/insights/2012/08/5-coolest-gov-cloud-projects/; https://aws.amazon.com/govcloud-us/;
- https://azure.microsoft.com/en-us/global-infrastructure/government/; and
- https://www.cio.gov/.

Active global providers

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

Generally speaking, all of them. The largest include AWS, Microsoft Azure, Google Cloud, IBM Cloud, and Salesforce.com; smaller providers (as measured by market share) include Rackspace, Oracle, NTT, Fujitsu, Alibaba and HP Enterprise. See www.zdnet.com/article/cloud-providers-ranking-2018-how-aws-microsoft-google-cloud-platform-ibm-cloud-oracle-alibaba-stack/.

Active local providers

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

Many of the 'local' cloud providers are the same as the global international cloud providers listed above. Although some global international cloud providers, such as Alibaba, do not have headquarters in the US, they typically have data centres and other operations in the US.

Market size

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

Cloud computing is very well established in the US. According to some projections, worldwide spending on public cloud offerings alone – of which the US market constitutes a material portion – is expected to increase from US$67 billion in 2015 to US$162 billion in 2020. The US federal government is expected to exceed US$10 billion in spending for cloud computing by 2023.

The largest players in public cloud offerings – particularly private data storage – are Amazon Web Services, Microsoft, IBM, Google, and Oracle. See:

- www.zdnet.com/article/cloud-providers-ranking-2018-how-aws-microsoft-google-cloud-platform-ibm-cloud-oracle-alibaba-stack/;
- www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#6eb471b931e8; and
- www.marketresearchmedia.com/?p=145.

Impact studies

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

There are many publicly available studies about the impact of cloud computing in the US. These studies indicate that the impact has been considerable and will continue to grow over the next five years. For instance, according to a cloud computing study by IDG Communications, 73 per cent of 550 surveyed organisations had at least one application or a portion of their computing infrastructure in the cloud; the average environment included 53 per cent non-cloud infrastructure and 23 per cent SaaS, 16 per cent IaaS, and 9 per cent PaaS resources; and more than a third of respondents felt pressure to migrate 100 per cent to the cloud (see www.idg.com/tools-for-marketers/2018-cloud-computing-survey/ and www.infoworld.com/article/3297397/cloud-computing/cloud-computing-2018-how-enterprise-adoption-is-taking-shape.html). As previously reported by Forbes, market intelligence firm IDC has stated that cloud computing is growing at 4.5 times the rate of IT spending since 2009 and is expected to grow at more than six times the rate from 2015 to 2020 (www.salesforce.com/assets/pdf/misc/IDC-salesforce-economy-study-2016.pdf).

As noted above, as cloud offerings are very rapidly becoming the default, legacy offerings such as on-premises solutions and traditional models of IT outsourcing are both less in demand and less available.

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?

Yes. Policy in this area tends to focus on moving government agencies to cloud services. One example is the Cloud First Initiative, launched by former US government CIO Vivek Kundra, which aimed to cut waste and increase efficiencies within the US federal government's technology services by reducing government IT expenditures by US$4 billion dollars over the next two years (www.wired.com/insights/2012/08/5-coolest-gov-cloud-projects/). As one result of this initiative, the General Services Administration, the federal government's procurement agency, has developed a number of resources to assist government agencies in procuring cloud services (www.gsa.gov/portal/content/190333). The current administration has continued these efforts by working to implement the Modernizing Government Technology Act, which has, as one of its goals, transitioning legacy IT systems to commercial cloud computing platforms, particularly platforms serving more than one covered agency with common requirements (www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf). And, in 2017, President Trump signed an Executive Order on cybersecurity mandating that federal systems move to the cloud (www.geekwire.com/2017/trump-cybersecurity-cloud/).

Incentives

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

In addition to the policies discussed generally above, certain development and government grants and other incentives promote technological investment, which increasingly means cloud services as a default. For example, the US federal government's Centers for Medicare & Medicaid Services established Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs to encourage eligible healthcare providers to adopt, implement, upgrade, and demonstrate meaningful use of certified EHR technology. The availability of these 'meaningful use monies' has spurned a lot of spending on EHR systems, which nearly always involve some cloud computing components.

LEGISLATION AND REGULATION

Recognition of concept

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

From a legal perspective, cloud computing is principally dealt with in commercial contracts and, therefore, governed by contract law, which is generally a matter of state law (as opposed to federal law) in the US. Additionally, cloud computing implicates numerous federal and state laws drawn to specific related topics or issues, including data security laws, data breach and notification laws, data transfer laws and various data-specific regulations, like those addressing the processing, storage and use of healthcare information, financial transaction information and other confidential information. These laws are addressed in more detail in the sections below.

Governing legislation

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

We are not aware of any laws or regulations that 'directly and specifically prohibit, restrict or govern' cloud computing. However, there are numerous federal and state laws that indirectly impact cloud computing services, as discussed further below.

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

While we are not aware of any laws or regulations specifically addressing cloud computing per se, there are numerous federal and state laws that indirectly impact cloud computing services.

State privacy laws

Generalised data privacy and data breach notification laws in the US are generally a matter of state law (as opposed to federal law). All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands now have specific breach notification laws (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx). These laws differ in significant respects as to how and when notification requirements are triggered, and whether and how cloud computing is implemented in any given scenario affects how these laws are applied to determine parties' rights and obligations.

Federal privacy laws

There is no comprehensive US federal law regarding generalised data privacy or security or data breach notification. Instead, there are various sectoral federal laws imposing regulation on data security for certain types of information, including information that is often stored in the cloud.

Certain US regulatory frameworks require data owners to ensure that their third-party service providers are capable of maintaining the privacy and security of personal information entrusted to them. This is typically accomplished through the use of contractual provisions mandating particular security measures. Three federal privacy laws that restrict the activities of service providers are the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191; the Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338, codified in relevant part at 15 U.S.C. §§6801-6809 and §§6821-6827; and the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99.

Health Insurance Portability and Accountability Act (HIPAA)

Under HIPAA's Privacy Rule, an entity may not use or disclose protected health information (PHI) except as permitted or required by the Rule, or as authorised in writing by the individual affected. HIPAA's Security Rule complements the Privacy Rule and deals specifically with Electronic PHI. This Rule lays out three types of security safeguards required for compliance: administrative, physical and technical. The Rule identifies various security standards for each of these types. Required specifications must be adopted and administered as dictated by the Rule. The HITECH Act provisions are also applicable as they have expanded and enhanced HIPAA privacy and security rules.

Further, any HIPAA-covered entity would first have to negotiate and enter into a business associate agreement with a cloud provider before the cloud provider could store records containing PHI in a cloud computing facility as such cloud providers would be 'business associates' under HIPAA. In some cases, HIPAA's substantive requirements

could conflict with the cloud provider's operations or terms of service, and a covered entity would risk a HIPAA violation by using such a provider to store or process PHI.

The Gramm-Leach-Bliley Act (GLBA)

For entities subject to the GLBA, the use of a cloud provider would be subject to similar restrictions. The GLBA's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties. Any such disclosures that are permitted under the GLBA are subject to numerous restrictions under both the Privacy Rule and Safeguards Rule. Pursuant to the Privacy Rule, prior to disclosing consumer personal information to a service provider, a financial institution must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Under the Safeguards Rule, prior to allowing a service provider access to customer personal information, the financial institution must: (i) take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards (ie, the entity must undertake appropriate due diligence with respect to the service provider's data security practices); and (ii) require the service provider by contract to implement and maintain such safeguards.

Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects student personally identifying information collected by educational institutions and associated vendors. These institutions must have the student's consent prior to disclosure of personal data, including grades, enrolment status or billing information. FERPA does not prohibit the use of cloud computing solutions for the purpose of hosting education records; rather, FERPA requires schools to use reasonable methods to ensure the security of their IT solutions, which includes cloud providers.

Also, although not a US law, the EU's General Data Protection Regulation is commonly interpreted to have a significant effect on the operations of US entities and interests, which effect often implicates use of cloud computing resources to collect, process, and store personal information (www.businesswire.com/news/home/20180815005111/en/Gartner-Survey-Cloud-Computing-Remains-Top-Emerging).

In addition to official laws and regulations, there are certain industry standards implicated by cloud computing that are so commonly adopted and implemented that they are treated effectively as official regulations would be in a commercial transaction. For example, the Payment Card Industry Data Security Standard (PCI DSS), which is referenced as a standard by some state laws, was jointly developed by payment card companies to simplify compliance for merchants and payment processors. It has six core areas and 12 requirements that cover best practices for, for example, perimeter security, data privacy and layered security. As a practical matter, any cloud-based application that processes payment card transactions typically must comply with PCI DSS.

Breach of laws

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

Violation of the laws and regulations identified above are typically addressed by fines and penalties, which can be significant, particularly if tallied on a per violation basis across any appreciable volume of business. For example, violations of HIPAA's data security provisions can range from US$100 per violation for an unknowing violation to fines of US$250,000 per violation and imprisonment up to 10 years for the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm. See:

- www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html; and
- www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Consumer protection measures

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

We are not aware of any consumer protection measures specific to cloud computing, but general consumer protection measures could apply to cloud computing products and services (eg, cooling-off periods, implied warranties covering quality and performance, restrictions on excluding and limiting liability, dispute resolution and venue for proceedings in the consumer's jurisdiction, governing law and other mandatory or overriding local laws for the benefit of the consumer). These protections are typically a matter of state (as opposed to federal) contract and consumer protection laws and enforcement actions and initiatives of state attorneys general (ie, the chief lawyers and law enforcement officers in each state) and vary from state to state.

At the federal level, consumer protection generally is handled by the Federal Trade Commission (FTC). The FTC has broad jurisdiction to regulate unfair or deceptive acts or practices in or affecting commerce. In the area of cloud computing, the FTC is most concerned with issues of privacy and security of consumer data.

Sector-specific legislation

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

As discussed in more detail above, relevant federal laws in particular tend to be sector-specific: the GLBA and PCI DSS are relevant to the financial sector, HIPAA and HITECH are relevant to the healthcare sector, and FERPA is relevant to the education sector.

Insolvency laws

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

We are not aware of any insolvency laws that apply specially to cloud computing. In practice, the issues that typically arise in this context are whether and to what extent data held on third-party servers are 'assets' of a debtor subject to the automatic stay that generally halts actions by creditors to collect debts from the debtor. For example, different questions arise when a cloud service provider files for bankruptcy (eg, is third-party data held on its servers part of the bankruptcy estate or how does the third party who owns the data recover it) versus when a data owner files for bankruptcy (eg, can a non-debtor cloud service provider delete or alter the debtor's data unilaterally or does it need relief from the bankruptcy court to do so?).

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.

As discussed above, at the federal level, data protection and privacy legislation is addressed sectorally, by laws such as HIPAA, GLBA and FERPA. Additionally, the Children's Online Privacy Protection Act

is a federal law enforced by the FTC that governs the online collection of information from children under the age of 13. See www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

State laws typically address data protection and privacy more generally, with laws varying from state to state. As noted above, many states have data breach notification laws. Other relevant state laws include

- the California Online Privacy Protection Act, Delaware Online Privacy and Protection Act, and the Nevada online policy law, which, among other things, require online services to post a privacy policy;
- the California Shine the Light law, which, among other things, addresses the practice of sharing personal information of consumers for marketing purposes;
- the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, which, among other things, provides security requirements for organisations that handle private data of payment card residents;
- Illinois and Texas laws governing the collection and use of biometric data; and
- the Illinois Geolocation Privacy Protection Act.

Additionally, the California legislature passed a broad digital privacy law in 2018 as the first US law approaching generalised data regulation similar to that seen in the EU. This law is not set to go into effect until January 2020 and is expected to be modified before then, but it is likely to significantly change the landscape for generalised data regulation in the US (www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html).

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)?

Cloud computing contracts typically manifest in different forms and draw on different legacy contracts and precedents depending on the particular vendor, offering and customer. For example, cloud computing contracts can resemble legacy software licence agreements, legacy managed services or hosting agreements, and limited purpose outsourcing agreements. As cloud services become more and more commoditised, cloud computing contracts are increasingly being presented by vendors as click-wrap agreements that are little- to non-negotiable agreements or as otherwise negotiable agreements that have significant portions that are designated as non-negotiable (eg, links to click-wrap maintenance, warranty, service level, acceptable use and privacy terms).

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?

Governing law

It is common practice in the US to choose as the governing law of a B2B public cloud contract the law of the state where one of the parties is located, typically the vendor (ie, where the party is headquartered or has a principal place of business). The governing law provision typically also includes a specific statement that the named state's choice of law principles should not apply. This statement is important because one state's choice of law principles may mandate application of another state's laws under the circumstances, which would subvert the intent of choosing the state's law to apply. Also, it is common to include an express statement that the UN Convention on Contracts does not apply, usually because the parties are more familiar and comfortable with US case law. As an alternative to the law of the state where one of the parties is located, the parties may choose a neutral state's law to apply. Common choices for a neutral state with significant commercial contract case law include New York and Delaware.

Jurisdiction

It is common practice in the US to choose a specific city or county located within the state that was chosen for the governing law as having exclusive jurisdiction over a dispute relating to the contract.

Enforceability/cross-border issues

In cloud computing contracts, there are a number of cross-border issues, particularly relating to data protection laws.

Dispute resolution

Dispute resolution tends to include some mechanism for internal dispute resolution, which may be pro forma or more meaningful, followed by either arbitration or litigation. Whether the parties agree on arbitration or litigation depends on the parties' experiences and preferences.

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 (price, payment, etc) and acceptable use (AUP), and variation?

Price/payment

Typically there are subscription fees for the cloud service that are invoiced monthly. Certain professional services may be offered and are typically billed as a fixed fee or on a time and materials basis. Professional services could include implementation, integration, training, support, enhanced maintenance (beyond that covered by the subscription fees), customisation or data analysis.

Audits

Cloud agreements generally contain audit provisions to ensure compliance with billing or payment obligations. However, audits may also be directed to other issues, such as regulatory and compliance, quality, and security. The audit provision typically specifies parameters and limitations for the audit (eg, during business hours, once per year), use of a third-party professional, such as an accountant, confidentiality and limited use of results of an audit.

Insurance

Either party (most commonly the vendor) or, in some cases, both parties may be required to obtain and maintain specified levels of insurance during the term of the agreement (eg, commercial general liability, errors and omissions) and cyber insurance that specifically covers a data breach. These provisions typically require the other party to be provided with a certificate of insurance or the actual policy (to confirm scope of coverage) and to be named as an additional insured.

Acceptable use

Typical acceptable use restrictions include:

- personnel limitation can only be used by customer and customer's employees, and whether or not affiliates or subcontractors are included is negotiated;

- maximum number of users;
- no reverse engineering;
- internal business purposes only;
- no modifying or creating derivative works;
- no interference with use of the platform by other users;
- no testing the platform for vulnerabilities, regardless of motive;
- no use that infringes or violates the rights of third parties (eg, intellectual property or privacy rights);
- no use for an unlawful purpose;
- no use to harass, defame or abuse a third party; and
- no posting of obscene, profane, sexually explicit, violent, threatening or discriminatory content.

Often the cloud provider will include as a remedy its ability to suspend or terminate the service for any breach of the acceptable use restrictions.

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?

Data and confidentiality (generally)

Most cloud computing contracts include mutual confidentiality provisions. The definition of confidential information is categorical, but may include specific items each party wants to protect as confidential information (eg, the customer's data). Obligations of confidentiality typically survive termination or expiration of the agreement, and it is not uncommon for this survival to have a sunset (eg, five years after termination or expiration), with or without express carve-outs for trade secrets. In recent practice, the US federal Defend Trade Secrets Act requires certain language to be included in agreements to make clear that individuals may share confidential information with attorneys or with law enforcement in connection with whistle-blowing activities. Because this language must be included to preserve certain remedies in the event of a trade secret claim later, this language is more and more often being added to agreements that include confidentiality provisions.

Data integrity

Customers typically request an express statement that they own all their data and are only granting the cloud provider the right to access, use or manipulate the data as required to provide the cloud service. Cloud providers often want to have rights to aggregate and use customers' data; this is a point of negotiation in some cases.

Data preservation

Customers typically want their data backed up by the cloud provider, with visibility into the process and geography implicated by the back-up, and commitments (ie, warranties) regarding frequency, recovery point objective, recovery time objective and periodic restoration testing. Typically, upon termination of the agreement, cloud providers are obligated to promptly return all data to the customer, in an agreed-upon format (preferably a standard format) or to certify destruction in writing after return of the data and confirmation by the customer that the data are accessible.

Premises and data security

This can vary widely. For data centres, customers look for electrical sources and generator backups, cooling, humidity and temperature controls, internet connectivity, physical security (video cameras, locks and access badges, escorted visitors, security personnel stationed there), information security (firewalls, passwords, encryption, etc), maintenance and redundancy. Usually require third-party security audits such as SOC2 or SOC3.

Data disclosure

Data disclosure is typically limited only to employees or agents who have a 'need to know' for the purpose of the agreement and who have signed a confidentiality agreement or are bound by professional obligations of confidentiality.

Disclosures may only be made if required by law (subpoena, court order, etc) so long as the party that received the data provides notice to and cooperates with the party that disclosed the data to the receiving party so that the disclosing party can seek to fight the disclosure.

Location of servers and data

Customers typically want the data to stay in their jurisdiction (ie, stay inside the US) and commonly vendors will not be able to move the location of servers or data without prior written approval from the customer.

Cross-border data transfers

There are numerous laws and mechanisms governing cross-border data transfers. The most recent is the EU–US Privacy Shield.

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?

Representations and warranties

Typical representations and warranties in a cloud computing contract fall into three categories: ability to enter or perform the agreement generally, service-related and software-related.

The first category of representations and warranties is directed to the parties stating that they have the ability to enter into the agreement, they have all the rights necessary to grant the rights granted therein, they aren't under any pre-existing agreement that would limit their ability to perform this agreement, they will not enter into any agreement that would limit their ability to perform this agreement, and they will comply with all applicable laws (including data breach notification laws).

The second category of representations and warranties target the performance of services under the agreement. Generally, the vendor is required to represent and warrant that it will perform all services in a good and workmanlike manner, with qualified personnel having the skill required of the industry, it will replace any unsatisfactory personnel (if applicable) and re-perform any unsatisfactory services, and it will use its established, industry-standard methodologies to provide services. The vendor may also expressly warrant that it will meet its service levels.

The third category of representations and warranties target the software components of the cloud service. Typically the vendor will represent and warrant that there is no malicious code or virus within the cloud software, and that the software itself (and use of it) does not violate any third-party intellectual property right (eg, patents and copyrights). Open source representations and warranties may be appropriate or not depending on the offering.

Limitation of liability

The limitation of liability provision is closely connected to the indemnification provisions and addresses qualitative limits on type of damages and quantitative limits on amount of damages. The limit on type of damages typically excludes indirect, consequential, special, incidental and punitive damages and may expressly exclude lost revenues or profits, loss of use and loss of data. The limit on amount of damages can be set at a specific number or it can scale (eg, with reference to the amount paid or payable under the agreement (or some multiple thereof)) over a certain period of time. Typically, when the quantitative limitation of liability references amounts paid or payable over some period of time, there is also some reasonable floor to cover a significant

liability in the early part of the contract term when payments have not accrued sufficiently to cover such a liability.

Often there are exceptions to the limitations of liability for specific items, such as breach of an obligation of confidentiality or data security or privacy, indemnification obligations, misuse of intellectual property, bodily injury (including death) and injury to personal or real property (not unusual to see, but less likely to be relevant in a cloud computing agreement), fraud, gross negligence or wilful misconduct. The parties typically will spend a lot of time negotiating the limit on liability exceptions. An alternative is to set a separate (often higher) limit for these items (rather than excepting them from any limitation of liability).

Indemnification

The indemnification provision typically includes an obligation to indemnify and hold the other party harmless for certain enumerated circumstances. Often the indemnification provision includes an obligation to defend, though this depends on the offering and the parties.

Indemnified parties are typically defined to include the parties to the agreement, their affiliates and their directors, officers, employees and successors. This list can be expanded to include subcontractors, suppliers, and customers, under certain circumstances.

The items for which a party (typically the vendor, but in some circumstances the customer) has an indemnification obligation in cloud computing contracts typically include:

- breach of the agreement (or, more specifically, breach of a representation or warranty);
- IP infringement claims;
- tort actions (ie, bodily injury, death or damage to personal property) due to acts or omissions of a party;
- fraud, gross negligence and wilful misconduct;
- breach of confidentiality;
- breach of data security provisions or data breach; and
- violation of law.

Also addressed in the indemnification provision is the procedure for obtaining indemnification, including terms for notice, cooperation and the right to participate in the defence.

Service-level agreements (SLAs)

SLAs typically address availability (uptime), latency, incident response times and work levels until resolution, and backup and restoration procedures.

The single most common SLA is availability, and some vendors, if they offer any SLAs, will offer only an availability SLA. It is common for a vendor to qualify an availability SLA with a commitment to use 'commercially reasonable efforts' to achieve a stated availability (though this is often objected to by the customer). The availability SLA commonly has exclusions for scheduled and emergency maintenance and force majeure events, and specific notice and reporting to customer in preparation for downtime. Customers will want vendors to self-monitor and report compliance with SLAs to the customer, whereas the vendor will want customers to have to monitor (or 'feel') and report suspected SLA failures to the vendor.

Often the remedy for a breach of an SLA will be limited to the vendor providing a service credit to customers.

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?

IP ownership

Typically, the cloud vendor owns the software underlying the cloud computing services and any software the vendor makes available for direct use by the customer. The customer typically owns all its data and provides a licence right to the cloud vendor to access and use the data as needed to provide the service.

If there is any development work or customisation work, the parties typically negotiate ownership rights. Typically, the customer will own all right, title, and interest in and to all work product created under the agreement specifically for the customer, and the vendor will name the customer as 'the person for whom the work is prepared' and designate the work product as a 'work made for hire'. The vendor should also assign all of its right, title, and interest in and to such work product to the customer, in case any work product does not meet statutory requirements to be a 'work made for hire', and provide further assurances from itself and its employees as necessary to vest ownership rights in customer. Typically, the vendor will also give a licence to any of its background technology that is used in the work product.

IP infringement

As discussed above, IP infringement is typically addressed via a representation and warranty that there is no infringement or by an indemnification obligation for third-party IP infringement claims.

Typical terms covering termination

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

Termination for cause

There is typically a mutual right of termination for cause (ie, for a material breach of the agreement by the other party that has not been cured for a certain period of time since notice of the material breach, eg, 30 days). The parties may specifically identify certain breaches that are deemed material breaches in order to forgo any dispute over materiality later. For example, the customer may seek an express termination right if the vendor catastrophically fails to meet an availability SLA.

Termination for convenience

Often the customer will want a termination for convenience clause, which allows the customer to terminate the agreement at any time and for any reason, upon written notice to the vendor. A termination for convenience right can greatly help to mitigate a customer's risk in a contract. Vendors very commonly object to a customer's right to terminate for convenience. Often, for a vendor to accept a customer's right to terminate for convenience, there is typically a liquidated damages term (ie, an early termination fee). The amount of the fee varies.

Survival of terms

The parties typically stipulate which provisions survive termination of the agreement. Often, the parties want terms for confidentiality, IP ownership, dispute resolution, limitations on liability and indemnification to survive termination.

Transition services

The customer typically will seek some level of transition services upon expiration or termination of the agreement, which typically includes an extension of cloud services for a set time after termination, such as

30–90 days, so that the customer will still have access to the cloud solution while it transitions to a replacement provider. Transition services typically also include a provision that the vendor will cooperate as necessary with the replacement provider in order to assist with the transfer of the customer's data and operations.

Effect of termination

The parties typically include in an 'effect of termination' provision terms that require the return or deletion of all data and confidential information of the other party, and transfer of all deliverables, whether complete or in progress, from the vendor to the customer.

Employment law considerations

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

There is typically a provision that states that the parties are independent contractors and not in an employment or joint venture relationship, with an express statement that neither party has the ability to bind the other party. Less common is a provision that distinguishes between working hours and non-working hours for non-exempt employees under the Fair Labor Standards Act.

TAXATION

Applicable tax rules

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

In general, taxation is divided into income tax issues, gross receipt tax issues and sales tax issues. As applied to taxation of cloud computing offerings, the nexus for each category of issues may be different, and how to calculate the tax impact of a certain offering varies for the type of tax and the tax authority involved. For example, as a sales tax, a city such as Chicago might tax cloud usage depending on the type of usage by classifying it as a remote taxable lease, whereas a city such as New York might classify certain cloud usage as a non-taxable service, certain cloud usage as a taxable remote lease and other cloud usage as a taxable information service.

Some of the considerations that affect these issues include the ownership of intellectual property in the cloud; the locations of the vendor and the customer; different tax authority definitions applicable to the cloud offering or the business model under which the offering is made; how much of the offering can be characterised as a service versus tangible personal property; how much of the offering can be characterised as software versus goods and services; and whether implicated software is off-the-shelf versus customised.

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.

See question 24.

Amy Farris
aefarris@duanemorris.com

Manita Rawat
mrawat@duanemorris.com

Matthew Mousley
mcmousley@duanemorris.com

30 South 17th Street
Philadelphia, PA 19103-4196
United States
Tel: +1 215 979 1000

2475 Hanover Street
Palo Alto
California, CA 94304
United States
Tel: +1 650 847 4150

www.duanemorris.com

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 Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943) was enacted on 23 March 2018. The CLOUD Act amends the Stored Communications Act of 1986 (SCA) to allow federal law enforcement to compel US-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the US or foreign jurisdictions.

One of the motivating forces behind the CLOUD Act was *United States v Microsoft Corp.* In that case, federal law enforcement agents applied for a warrant requiring Microsoft to disclose all emails and other information associated with the account of one of its customers. Microsoft resisted the warrant because the account's email contents were stored in its Dublin data centre. The district court held Microsoft in civil contempt for refusing to comply with the warrant, but the appellate court vacated the civil contempt. The case was on appeal to the Supreme Court of the United States when the CLOUD Act was passed. With the enactment of the CLOUD Act, the government procured and served a new warrant pursuant to the new law, which the parties agreed replaced the original contested warrant. This replacement warrant rendered the parties' dispute moot, so the Court vacated the ruling on review and remanded the case with instructions to dismiss. See *United States v Microsoft Corp*, 138 S. Ct. 1186 (2018).

On 6 June 2018, IBM Corp and SAP SE announced plans to launch an edition of the SAP Cloud Platform running on the IBM Cloud for private cloud deployments. The companies said the collaboration would help clients in regulated industries build new applications in the

cloud without jeopardising security and control (www.ibm.com/blogs/cloud-computing/2018/06/06/ibm-sap-cloud-partnership/).

On 27 August 2018, Amazon and VMware introduced a version of Amazon's cloud-based database management software aimed at companies that use on-premises data centres. Amazon and VMware started working together on a combination of cloud and on-premises technology in October 2016.

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?

None.

* *The information in this chapter was correct as at October 2018.*

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
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
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
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
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
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 978-1-83862-164-3