Cloud Computing

Contributing editor
Mark Lewis

2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cloud Computing 2019

Contributing editor

Mark Lewis

Bryan Cave Leighton Paisner LLP

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

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

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2017
Second edition
ISBN 978-1-78915-001-8

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

CONTENTS

Preface

Cloud Computing 2019

Second edition

Getting the Deal Through is delighted to publish the second edition of *Cloud Computing*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

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 **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 new chapters on Argentina, Brazil, France and Korea.

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.gettingthedealthrough.com.

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.

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

GETTING THE DEAL THROUGH

London
October 2018

France

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

Market overview

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 which 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) (www.insee.fr/fr/statistiques/2646317?sommaire=2646324).

The different varieties of cloud computing services covered by this definition are offered in France. Accordingly, in 2016, the services the most frequently used were infrastructure-as-a-service (IaaS, according to the NIST typology), mainly in the form of file storage (21,974 companies out of the reportedly 31,687 using cloud computing). Software-as-a-service (SaaS) was also very frequently used by businesses, primarily for emails (19,464 companies). Database hosting was in third position (in the platform-as-a-service (PaaS) category). The other significant use of cloud computing included office automation software services and software for the management of client relations (source: Insee, TIC 2016 enquiry, TAB07: Use of the cloud computing service by internet).

Furthermore, according to the same statistical enquiry, in 2016 the companies that purchased cloud computing services on shared IT servers (public cloud) were almost as numerous as those that requested servers exclusively reserved for their needs (private cloud).

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

The principal global providers (Amazon Web Services, Microsoft Azure and Google Cloud Platform), for which the share of the world market is estimated at 57 per cent (www.lebigdata.fr/microsoft-azure-parts-marche-cloud, 30 July 2018), are very active in France. Numerous other international players commercialise their services directly or indirectly in the country (eg, IBM, Rackspace, Oracle, NTT, Fujitsu, Hewlett, Salesforce).

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, this market includes numerous less significant and more specialised players in France, including OVH, Cloudwatt and Ikoula (IaaS and PaaS) (which are listed with the principal global providers among the 10 leading providers in the CloudScreener/Cedexis/JDN ranking (www.journaldunet.com/solutions/cloud-computing/1167190-comparatif-cloud/). 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).

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

According to the official statistical enquiry undertaken in 2016 (see question 1), 31,687 companies (ie, 17 per cent of French companies with at least 10 employees) were using cloud computing services. This figure is compared with an average of 21 per cent noted in the countries of the European Union in that year.

On the information and communication technologies market, cloud computing services had a minimal representation in 2015, as the 'Data processing, hosting and related activities – internet portals' (according to the OECD classification, which stretches beyond the sole cloud computing services) only represented 4.8 per cent (ie, €3,281 billion) overall, in terms of added value (www.entreprises.gouv.fr/etudes-et-statistiques/numerique-chiffres-cles).

Nonetheless, the cloud computing market is rapidly evolving in France like elsewhere. An analysis undertaken by the research firm Markess estimated its annual growth at 21 per cent in 2017, with a total of €8.5 billion in turnover. This amount includes additional services provided in the form of consulting, support or assistance with the exploitation. SaaS represents 54 per cent of the total, closely followed by IaaS and PaaS (www.usine-digitale.fr/article/le-marche-francais-du-cloud-atteint-8-5-milliards-d-euros-en-2017.N645943).

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

Numerous analyses and official studies have been undertaken on the digital sector in France and, more specifically, on cloud computing services, although regular updating is still lacking. 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.

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). With regard to the users, associations such as Cigref (www.cigref.fr) or software user clubs such as SAP (www.usf.fr) also publish such analyses.

Policy

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?

During the past few years, the public authorities have encouraged the creation of data-hosting providers (such as Cloudwatt and Numergy) that can guarantee storage near customers' sites, on national territory ('sovereign cloud').

In 2018, they launched a strategy to encourage administrations, public establishments and local authorities alike to choose cloud computing among a variety of options including private cloud as well as public or hybrid solutions (www.numerique.gouv.fr/node/88147).

Furthermore, the government greatly strives to open its data to the public (www.data.gouv.fr). On this count, France is now ranked fourth globally (https://index.okfn.org/).

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

There are financial funding and tax benefits that may help support investments in cloud computing activities but are not reserved for them.

Specifically, financial funding for innovation and loans may be granted in the context of the Investment Plan for Europe (the Juncker Plan) and may be combined with national funding. The offers are accessible at 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).

The companies that invest in cloud computing may also benefit from preferential tax benefits such as tax credit on research and development costs, the tax exemption for innovative new companies or the tax credit for innovation expenses.

Legislation and regulation

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 the term 'cloud computing' as 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 of this term in the French language (*informatique en nuage*).

Law No. 2018-133 26, dated 26 February 2018, defines the 'cloud computing service' as 'a digital service that enables access to a set of flexible and variable IT resources which may be shared' (which could restrict cloud computing to IaaS and PaaS services). This service is classified among the 'digital services', along with online marketplaces and search engines, for which the providers are obliged to comply with certain security obligations (see question 9).

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

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 – network and information security). This is the sole text which, to date, directly and specifically monitors cloud computing services in France.

This law obliges 'digital service 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 of France (ANSSI) of any incident which 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 authority. 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.

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)

French law distinguishes the activities relating to 'content' accessible online (eg, user platforms, search engines, site hosting, portal management, edition of online content, etc) from telecommunication services, which concern the 'container'. For example, the telecoms operators are not classified among the 'digital service providers' (see question 9).

Nonetheless, in practice, the boundaries are not as clearly defined. On the one hand, the telecoms operators offer cloud computing services. On the other, the content providers are more and more seeking to bring their content closer to the end clients and set up cache servers in the operators' networks. Accordingly, in France, about 50 per cent of the incoming traffic to telecommunication service providers originate from the four main content providers – Google, Netflix, Akamai, Facebook (source: Regulatory Authority for Telecommunications (ARCEP), 2018 Report). This reflects a highly condensed market.

Yet, the telecoms network operators and the telecommunication service providers are subject to obligations specific to them, but which could or should also concern cloud computing services, such as the principle of internet neutrality (governed by (EU) Regulation No. 2015/2120 dated 25 November 2015), the protection of personal data, the protection of confidentiality of correspondence and the neutrality with regard to the content of the messages communicated (CPCE, article L32-1). Also, telecoms operators are obliged to ensure the conservation of technical communication data for the needs of the prosecution of criminal offences and the fight against terrorism.

Finally, 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 the 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, including the seizure of data hosted on IT servers. The location of servers abroad does not constitute an impediment (Paris Court of Appeal, Division 5, Chapter 7, Order dated 31 August 2012).

Others
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, 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 in France.

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 five-fold for the operators as legal persons.

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 French 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), prohibited or regulated commercial practices and abusive clauses, 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 an 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 General Data Protection Regulation (GDPR) (see question 15).

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 (RGS), 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). So far, no cloud computing service provider has fulfilled the criteria to be considered as a 'qualified service provider'. The ANSSI often underlines that the cloud computing services' compliance with the RGS – and beyond with the security policy enacted for the state's information systems – must not be taken for granted.

Public Estate Code (public sector)
The Public Estate Code defines the legal regime for state archives and public entities 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. New criteria for such certification are currently being defined by the public health agency (ASIP Santé). Failure to meet such requirements 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 (ie, 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).

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

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 is being supplemented by national legislation based on the former law of 6 January 1978, which is still pending finalisation at the time of writing.

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). Nonetheless, 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 (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, provided 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 transferred to any country where access to such data is technically possible: the location of the servers is therefore not sufficient to determine whether a cross-border transfer is taking place or not. 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

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.

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 their 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.

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.

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 and/or storage for clients' data and purport to be 'content agnostic', cloud service providers which 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 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: this is not limited to the country where data is stored, but applies to all the countries where 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.

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 commercially 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 telecoms 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 compensate 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 only 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).

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 rightsholder 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.

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.

Update and trends

The software publishers strongly recommend their clients replace their on-premise applications by cloud computing services (SaaS), which allow for economies of scale but tend to make the clients more dependent. The underlying hosting market (IaaS) progressively covers nearly all IT services. This trend raises questions about the risks related to the concentration of this market to a few global players.

The research firm Gartner expressed this concern early in 2018: 'The increasing prevalence of the IaaS hyper-scale providers create both enormous opportunities and challenges for the end users and the other market players . . . The companies should be cautious concerning the uncontrolled influence of the IaaS providers on the clients and the market' (www.solutions-numeriques.com: cloud-public-une-croissance-du-marche-mondial-de-214-en-2018-liaas-en-progression).

The record fine of €2.42 billion issued on 27 June 2018 by the EU Commission to Google for having abused its dominant position on the search engines, with a view to benefiting its price-comparison engine and downgrading those of its competitors in the users' search results shows the risks entailed by this type of dominant position (www.huffingtonpost.fr: lunion-europeenne-inflige-a-google-une-amende-record-de-2-4-mil_a_23003706/).

The GDPR (see question 15) opens the door for a number of subjects to be varied or adapted at the national level. Legislative and regulatory initiatives should be monitored throughout the coming year.

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

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

Despite the recurring trend for the implementation of sectorial taxes on companies or digital services (eg, tax on bandwidth or the data exchanged), the cloud computing service providers are currently subject solely to the standard corporate tax, at 33.33 per cent. This rate will 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, and in particular, the redefinition of the notion of fixed establishment.

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 the cloud computing services entails complexity, 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

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 presents a significant challenge for the business model used by the 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.

Nanterre Tribunal de grande instance, interim order, 30 November 2012, *UMP v Oracle*
This former case is still an important reference in the area of cloud computing as it addresses reversibility issues, which rarely come before the courts. The claimant was a political party that had subscribed to a SaaS provider for the management and hosting of the database of its adherents. As it intended to revert to another IT provider upon the expiry of the contract, the party tried to recover its data, but the exportation tool set up by Oracle was not working. The court ordered the provider to provide the necessary means for this exportation immediately, or to guarantee the extension of its service without cost for two months beyond the date on which the exportation would become possible (www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-nanterre-ordonnance-de-refere-30-novembre-2012/).

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

Getting the Deal Through

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
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
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
Loans & Secured Financing
Mediation
Merger Control
Mining
Oil Regulation
Outsourcing
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-Private Partnerships
Public Procurement
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
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-001-8