LEXOLOGY®
Getting The Deal Through

Cloud Computing

in France

Report generated on 19 November 2020

Table of contents

RECENT CASES

Notable cases

UPDATE AND TRENDS

Key developments of the past year

Coronavirus

LAW STATED DATE

Correct on

Contributors

France

Jean-Luc Juhan
jean-luc.juhan@lw.com
Latham & Watkins LLP

LATHAM & WATKINS LLP

Myria Saarinen
myria.saarinen@lw.com
Latham & Watkins LLP

MARKET OVERVIEW

Kinds of transaction

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

INSEE, the National Institute of Statistics and of Economic Studies publishes official statistics on Cloud Computing in France every two years. According to the most recent studies published in 2018, about 19 per cent of entities with 10 or more employees subscribe to paid cloud computing services. These cover the full range of available cloud services including infrastructure-as-a-service (IaaS), software-as-a service (Saas), as well as platform-as-a-service (Paas). The most commonly used paid cloud service in France was data-storage, with about 77 per cent of the companies using paid cloud services subscribing to data hosting. SaaS subscriptions, in particular for email and office software were common among businesses as were PaaS subscriptions focused on database hosting services. Both public and private cloud computing, as well as hybrid cloud models are used.

In April 2020, Microsoft Azure won the public procurement bid for the hosting of Health Data Hub, the French public health data warehouse. This decision was criticised and was subject to challenges before the French Supreme Administrative Court that were subsequently rejected.

Active global providers

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

The French cloud market share closely tracks the global market share, with international entities occupying dominant positions across SaaS and PaaS .

Salesforce, Microsoft, ADP, Oracle and Adobe are the top five providers in terms of market share for SaaS. Microsoft, Amazon Web Services, Salesforce, IBM and Google dominate the PaaS market. As of 2018, Microsoft Azure and Google Cloud had data centres physically located in France. Other global actors such as Alibaba and Xiaomi also offer cloud services in France. Tencent announced its entry into the French market by the creation of SAS Tencent Cloud Europe headquartered in France , becoming the last of the key Chinese players to enter the French cloud market as of September 2020.

Active local providers

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

Although lagging behind international entities when it comes to SaaS and PaaS, French entities are maintaining a solid position in the IaaS market within France. French entities such as OVH Cloud, Claranet, Outscale (a subsidiary of Dassault Systèmes) and Linkbynet are closely following Amazon Web Services in the IaaS market.

Other local providers such as Capgemini, Atos, Orange Business Services and Sopra Steria are also maintaining top five positions alongside IBM for integrated cloud services offerings including outsourcing and technology services.

EuroCloud France , the French branch of the pan-European cloud provider organisation EuroCloud , has 108 publicly listed members covering all aspects of cloud services as of September 2020.

Market size

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

Despite its steady development, the French cloud market remains slightly underdeveloped in comparison to the European market. According to official statistics published by the INSEE in 2018, paid subscription to cloud services among companies with more than 10 employees are lagging about 5 per cent behind the EU average.

Nonetheless, a report published by the International Trade Administration estimates the French cloud market to be worth over US$11 billion in 2018, with a growth rate of 23 per cent between 2017 and 2018. The public cloud market, in particular, was estimated to have grown by 49 per cent during the same period. In another study published by Markess , a research firm, the size of the French cloud computing market was estimated to reach €12 billion in 2019, representing a 20 per cent growth from 2018.

Impact studies

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

The INSEE publishes data regarding cloud computing every two years on both the French and European levels. The French Senate and General Assembly regularly commission reports regarding the digital economy. For example, a 2019 report by the French Senate on Digital Sovereignty includes a section on cloud computing and its development. The Ministry of Economy and Finance also publishes studies regarding the digital economy including the impact of cloud computing and big data, with a focus on the provision of guidelines for public bodies in their adoption of cloud computing services .

Professional organisations and industry bodies such as EuroCloud France or CIGREF (French association of large enterprises and public administrations) also publish public reports and analyses on cloud services and their impact on the market.

POLICY

Encouragement of cloud computing

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?

Encouraging the development of the digital economy at large has been one of the key objectives of the current administration. The development of local cloud services has been part of this larger policy. Historically, the perceived threat of global actors and the loss of digital sovereignty has pushed administrations to encourage and reinforce the development of local start-ups and technology service providers. For example, in 2009, the government spearheaded the concept of ‘French Cloud’, which resulted in the investment of €150 million for the creation of two data hosting providers, Cloudwatt and Numergy, in 2012. Currently, discussions around the establishment of a government-sponsored ‘trusted cloud’ are under way. France has also positioned itself, alongside Germany, as one of the main sponsors of GAIA-X, a proposal for a federated European data infrastructure.

Incentives

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

In addition to public-private partnerships that were undertaken for the development of Cloudwatt and Numergy, the French government has launched several initiatives to boost the development of local digital actors and small and medium enterprises. For example, in 2020, the government announced a US$4.3 billion plan for supporting start-ups through the 'La French Tech' initiative. A new initiative with a funding of up to €500 million to bolster the development of tech companies and to mitigate the impact of the covid-19 crisis has been announced in June 2020.

Preferential tax benefits regarding investment in digital innovation, tax credits for research and development, and exemptions for new companies also aim to contribute to the development of tech companies including cloud computing providers.

LEGISLATION AND REGULATION

Recognition of concept

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

The concept of cloud computing has been introduced in official texts in 2010 by the Commission on Terminology and Neologisms as vocabulary specific to information technology and the Internet. According to this definition, 'cloud computing' is a 'method of processing client data, the exploitation of which is done via the internet, in the form of services provided by a service provider'. It is also noted that cloud computing is a 'specific form of information management under which the location and functioning of the cloud are unknown to the clients'.

In February 2018, a statutory definition of 'cloud computing service' was adopted by the Law No. 2018-133 implementing the European Network Information Security Directive (NIS). According to this definition, 'cloud computing service' is 'a digital service enabling access to a set of modular and variable information technology resources that can be shared' and is classified as a 'digital service', along with online marketplaces and search engines.

Governing legislation

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

The primary obligations specifically applicable to cloud computing result from the transposition of the NIS Directive through Law No. 2018-133 of 26 February 2018 and its implementing regulations.

Cloud service providers must guarantee a level of information security adapted to the risk and adopt appropriate organisational and technical measures to minimise their impact and ensure the continuity of service. Cloud service providers offering services within the EU without being established in the EU must designate a representative with the French National Cybersecurity Agency (ANSSI) unless a representative has been designated with another European authority. In the case of a security incident, a declaration must be made with the ANSSI without delay. The Prime Minister may open investigations upon information that digital service providers including cloud service providers are not compliant with security obligations.

Under French law, any documents and data produced by public entities are classified as public archives at the time of their creation and assimilated to national treasures under the French Heritage Code. As such, such document and data

are only exportable outside of the national territory subject to temporary authorisation. However, this restrictive regime is expected to be reformed by May 2021 to comply with the European Regulation on the Free Flow of Data, which prohibits members states from imposing the localisation of non-personal data on their national territory unless justified by public safety grounds.

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

Telecommunication operators are governed by the French Posts and Electronic Communications Code (PECC) imposing additional security, neutrality, personal data protection, and confidentiality obligations. Although cloud service providers are not, strictly speaking, telecommunications operators, certain cloud services may fall under the perimeter of the PECC. For example, cloud services aiming to use the label 'electronic safe' must comply with the obligations under the PECC. The EU Electronic Communications Code, scheduled to be transposed into national law by December 2020, will extend the reach of certain provisions under the PECC to 'interpersonal communications services' including 'over-the-top' services such as Voice over IP and messaging software-as-a service (Saas) services, increasing the relevance of the PECC to SaaS cloud services.

The law of military programming of 18 September 2013 introduced the concept of Essential Operators (OIV), a category of economic operators subject to heightened information security obligations due to their strategic impact on national interest. The use of cloud services by such actors will be subject to additional security obligations under articles L. 1332-6-1 et seq of the French Defence Code.

Any cloud services involving the processing of personal data must comply with the obligations stemming from the European General Data Protection Regulation (GDPR) and the French Data Protection Act. In addition, business clients will need to be mindful of general obligations regarding the retention of accounting and tax documents under the French Tax Procedure Code and the General Tax Code.

Breach of laws

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

Non-compliance with security obligations under Law No. 2018-133 can be punished with a fine of up to €100,000. Violations of obligations related to the deletion or anonymization of traffic data and the conservation of technical data under the PECC may result in imprisonment of up to one-year and a fine of €75,000 as well as a prohibition to exercise a professional activity related to the offence of up to five years. Violation of security obligations under the Defence Code applicable to Essential Operator may be punished by a fine of €150,000.

If a legal person, such as a corporation, rather than a natural person is found in violation of these provisions, the maximum applicable fine is increased fivefold for all of the above-mentioned obligations. Additional penalties such as the prohibition to exercise a professional activity related to the offence and publicity measures may also apply.

Consumer protection measures

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

France has strict consumer protection laws that present a risk of elevated fines. The provisions of the French Consumer Code governs B2C contracts, including online services and platforms and impose obligations regarding,

among others, pre-contractual information, guarantees, and prohibition of abusive or aggressive practices.

In addition to the general rules applying to consumer contracts, cloud contracts are likely to be subject to specific provisions regarding contracts concluded at a distance or electronically. Contracts concluded at a distance must comply to additional protective measures regarding information obligations such as the provision of pre-contractual information in a format adapted to the means of communication (articles L. 221-1 and L. 221-2 of the French Consumer Code), the provision of a confirmation on a durable medium (article L. 221-13 of the French Consumer Code), and a system of a double-confirmation of the consumer's payment obligations if the contract is concluded electronically (article L. 221-14). In addition, contracts of which the value is superior to €120 must be stored for a period of ten years in a written form if said contract is concluded electronically. Although the right of withdrawal does not apply to cloud contracts, express consent of the consumer for service provision as well as an express renunciation of the right to withdrawal must be obtained under article L. 221-28 of the French Consumer Code.

Sector-specific legislation

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

In addition to additional security obligations applying to Essential Operators, various sector-specific obligations apply indirectly to cloud services, especially when it concerns public entities and actors operating in heavily regulated sectors such as finance or health. These obligations do not necessarily apply directly and explicitly to cloud services, but set out certain obligations and standards applicable to information security services used by these actors more generally.

Public entities are subject to the obligation to assess the risk and guarantee the security of the information systems they use, including cloud services. They must comply with a general security standard published by the French National Information Security Agency (ANSSI). The ANSSI has also adopted specific standards regarding cloud computing, the ' SecNumCloud ', under which a certification scheme is provided. Public entities also have an obligation to maintain the stability and independence of their information systems and are encouraged to use free and open source software.

Additional security obligations and standards exist in the domain of national defence as adopted by the Decree of 30 November 2011 and in the energy sector under article L. 111-73 of the French Energy Code. Actors in the financial sector must ensure that cloud computing services comply with the rules governing outsourcing of activities as set out in Decree of 3 November 2014 regarding the internal control of companies in the banking sector and others. Finally, the French Public Health Code prohibits the provision of health data hosting services by operators who have not been certified by the French Digital Health Agency. In addition, any digital services and tools used by medical professionals and in medical establishments must comply with interoperability standards set by the French Digital Health Agency .

Insolvency laws

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

No specific provision regarding insolvency applicable to cloud computing service providers exist. The general provisions regarding insolvency and bankruptcy under the French Commercial Code apply to cloud computing service providers. A reversibility clause guaranteeing the restitution of the client's data in an exploitable form should be carefully negotiated considering the potential impact of the cloud service provider's disappearance without restitution of data.

DATA PROTECTION/PRIVACY LEGISLATION AND REGULATION

Principal applicable legislation

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

The GDPR as supplemented by the French Data Protection Act (Law No. 78-17 of 6 January 1978 on information technology, files and freedoms and its implementing acts, Ordonnance No. 2018-1125 of 12 December 2018, and Decree No. 2019-536 of 29 May 2019) govern the processing of personal data in France. Specific obligations arising under the French Data Protection Act apply whenever the data subject resides in France.

The main obligations applying in France regarding personal data processing, including cloud computing services, arise from the GDPR. As such, the principles of data protection including data minimisation, transparency, lawfulness, accountability apply to any cloud computing involving the processing of personal data. In the context of cloud computing, particular attention must be paid to the qualification of parties to negotiate and conclude proper contractual provisions including ensuring compliance with security obligations, guaranteeing the rights of data subjects, notifying data breaches, and ensuring proper governance of data transfers outside of the European Economic Area (EEA).

Although the service provider will be considered a data processor acting under the express instructions of the client who defines the purpose and method of data processing as a data controller for most service contracts, a factual analysis should be conducted in order to determine the proper qualifications as cloud computing service providers may be considered joint controllers due to their high level of autonomy, control over the methods of processing, and visibility in relation to the data subjects. Appropriate data processing agreements and allocation of responsibilities regarding the exercise of data subjects' rights should be implemented in consideration of the qualification of the parties.

The transfer of personal data to a country outside of the EEA must have a legal basis and only be carried out if sufficient guarantees ensuring a level of personal data protection equivalent to that in the EEA are put in place. The transfer of data outside of the EEA is a particularly thorny topic at the moment due to the recent invalidation of the Privacy Shield by the European Court of Justice . Cloud computing service providers transferring personal data to the US should pay close attention to personal data protection and data transfer agreements in order to provide sufficient guarantees.

Although prior to the entry into force of the GDPR, the French Data Protection Authority, the CNIL, has issued recommendations regarding business clients using cloud services in 2012 . As the CNIL is considered a relatively active data protection authority, cloud service providers processing personal data should be mindful of these aspects.

CLOUD COMPUTING CONTRACTS

Types of contract

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

In France, cloud computing contracts are generally drafted as service contracts. Often, a standard contract will be presented by the cloud service provider to the potential client. Cloud service contracts typically include clauses defining the object of the contract setting out detailed definitions of specific services to be provided even if a service level agreement is included as an annex. Standard contractual clauses including but not limited to intellectual property, confidentiality, audit, penalty, termination, reversibility, jurisdiction and applicable law clauses are also be included in the contract.

Key documents such as an acceptable use policy (AUP), general and specific terms and conditions, data processing and data transfer agreements, and a service level agreement (SLA) describing the quality, modalities and availability of service and key performance indicators (KPI) are often included as annexes that form an integral part of the contract. As under French contract law, an obligation that is impossible to achieve will cause the nullity of the clause, unrealistic service levels such as 100 per cent availability should be avoided.

Under French contract law, a contract including non-negotiable standard clauses are considered 'adhesion contracts' and are subject to particular scrutiny by the courts should they be subject to litigation. Clauses considered as creating a significant imbalance between the contracting parties' rights and obligations may be struck out by courts. In addition, courts interpret adhesion contracts against the drafting party as a principle. As a large portion of cloud service contracts fall under this definition, particular attention should be paid in order to avoid such situations.

Typical terms for governing law

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?

An applicable law and jurisdiction clause designating the client's place of establishment is typically included in cloud service contracts because of the uncertainty regarding the localisation of data centres and the multi-jurisdictional nature of cloud computing services.

Unlike in B2B contracts, jurisdiction clauses in B2C contracts may be considered abusive and struck down by the courts. In the absence of any contractual provisions, the law of the domicile of the consumer shall apply as long as the professional is established in or directs its activities toward the domicile of the consumer. The service provider can be sued before the courts of the jurisdiction in which the consumer is domiciled.

Typical terms of service

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?

Due to the highly variable nature of cloud computing services, contractual provisions strive to clearly define the perimeter of intervention. A clause outlining the nature of the service (hosting, provision of online solutions, connected services such as data management, development of custom software, maintenance, etc), type of the cloud (public, private, hybrid) and the resources and equipment provided to the client (server capacity, computing power) is typically included. The price is determined and invoiced periodically based on the services and resources provided.

Inclusion of an AUP limiting the possible uses of the cloud services to a set of identified purposes (eg, the client's internal business purposes) and prohibiting the use of cloud services for unlawful purposes or in violation of third party rights is standard practice for cloud computing agreements. The client generally undertakes to ensure the compliance with the AUP by its employees. Such policies may include the service provider's right to investigate suspicious use and to suspend client access in the case of violation of the AUP.

The obligation to adopt and maintain security policies on the client side are also typically included in cloud computing agreements to ensure that the data provided to the cloud provider meet a certain standard and are not illicit.

Typical terms covering data protection

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

Subscription to a cloud computing service implies that the service provider will be processing personal data. In consequence, confidentiality and data protection clauses are standard features of cloud computing contracts.

Typical confidentiality clauses include the acknowledgement, by the service provider, of the confidential character of the information and the processing activities subject to the contract. The clause limits the service provider's access to the data beyond what is strictly necessary for contract performance and stipulates that the service provider undertakes to limit employee access to data and to guarantee that they will preserve the confidentiality of client data. Security obligations in line with the cloud service provider standards of the ANSSI can be included in the confidentiality clause. Sectorial obligations such as the applicability of professional secrecy and trade secret protections should also be considered in the drafting of confidentiality clauses.

Data protection clauses setting out and adapted to the qualification of the parties are typically concluded alongside the confidentiality clause. When the cloud computing service provider acts as a data processor, the data protection clause must meet the requirements of GDPR article 28. Such a clause should include, among others, an engagement that the service provider will process personal data only on documented instructions from the client, the modalities for communicating and documenting such instructions, commitment to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, cooperation with the client for data subjects' rights exercise, and the duty to inform in the case of data breach. If a data processor further sub-contracts activities involving personal data processing, such engagements must be subject to the authorisation of the data controller. The data protection provisions as set out in the initial contract must be imposed on the subsequent processors through contractual or other legal means. If the parties qualify as joint controllers, the data protection clause must meet the requirements of GDPR article 26: allocation of responsibilities under relevant data protection laws should be carefully delineated, especially in light of data subjects' rights.

Provisions regarding data transfers should be included in data protection clauses, contractually setting out that personal data will not be transferred outside of the EEA absent the express authorization of the client and subject to adequate guarantees.

Typical terms covering liability

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

Owing to the highly technical nature of cloud computing services, the provider will be held, in addition to good faith, to a duty to advise, inform, and warn the client as necessary. In addition to these general obligations, the detailed definition of services including SLA ad KPI are drafted such that the obligations can be identified as an 'obligation of results' under French law, to provide greater certainty and protection to the business client, as the performance of a service provider held to an obligation of results will be assessed in relation to the accomplishment of a set outcome, in contrast to the 'obligation of reasonable efforts' under which the service provider merely needs to demonstrate that reasonable efforts have been made. Reversibility or restitution clauses that are solely under the responsibility of the service provider and of which a definite result can be obtained are often included to clearly impose an obligation of results. Quality and availability of services will typically be drafted as obligation of best efforts. In the case of dispute, courts will generally consider the level of uncertainty inherent to the obligation, the level of client involvement, control of the service provider over the supply chain, and known risks to determine the type of obligation.

Penalty clauses for delays and non-availability of service are generally included in cloud service agreements, with the penalty fixed at the delay or duration of unavailability multiplied by a percentage of the contract price (often payable as a service credit) to be applied at invoicing.

Limitation of liability clauses strictly restricting potential liabilities are common due to the market power of large global actors and the prevalence of adhesion contracts. In the case of adhesion contracts, such clauses, if deemed to create a significant imbalance, may be voided by the courts. Furthermore, limitation of liability clauses may be struck out if the court considers that such clauses exonerate the obligor of its essential obligations.

Typical terms covering IP rights

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?

Two types of IPR clauses are commonly included in cloud computing contracts. The first type of clauses set out exclusive ownership of IPR such that the client remains the sole owner of any data or third-party programs stored with the cloud service provider, whereas the service provider retains all IPR over any materials or software involved in the provision of services. The second type of clauses concern licences for the use of software provided as part of the cloud computing services, including licences for software customised or developed for the needs of the clients. In the case of third-party software, a sublicense should be provided. The IPR clauses should carefully set out the parameters of the licences and acceptable uses.

Finally, warranty of peaceful enjoyment clauses for the indemnification of each parties against third party infringement claims are typically included. Standard cloud contracts often include a clause authorising termination of services in cases where the client has infringed third-party rights. Clauses exonerating the service provider in the case of the client's storage of infringing material could also be negotiated.

Typical terms covering termination

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

Cloud computing agreements in France are generally concluded on a fixed-term basis. Careful negotiation of duration is recommended, with particular attention to be paid to advance notice periods and the applicability of provisions regarding sudden termination of contracts under the French Commercial Code, which may incur indemnities in the case of termination without sufficient advance notice if economic dependence or a severe impact on the client's activities can be proved.

Under French contract law, contracts can be terminated by the application of a termination clause, the notification of the party in breach in the case of a sufficiently material breach, or a court decision. Termination clauses should explicitly set out a list of conducts that will justify the termination of contract for breach.

Owing to the dependence of the client to the cloud service provider, and in particular the loss of control of data, reversibility clauses should be imperatively included and drafted with care to allow for the restitution and migration of data and other non-physical assets such as computer programs, specific developments for the clients, and proprietary data formats. Conditions regarding the cost of reversibility and technical specifications should be negotiated in order to avoid situations where the transfer and re-exploitation of data is made impossible due to technical limitations and other conditions imposed by the service provider. Finally, the reversibility clause should specify that it will apply regardless of the cause of the termination, including insolvability or disappearance of the cloud service provider.

If the cloud contract involves the processing of personal data and a data controller – data processor relationship, a contractual provision providing for the deletion or restitution of personal data upon termination should be included in accordance with article 28 of GDPR.

Employment law considerations

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

No specific labour and employment law provisions targeting cloud computing exist under French law. However, articles L. 1224-1 and L. 1224-2 of the French Labour Code impose a direct transfer of employment contracts whenever there is a transfer or change in the employer's legal status through operations such as mergers, acquisitions and transfers. The employment contract of the employee is preserved through the substitution of the former employer by the new entity as contracting party. Although these provisions are not automatically applicable to business customers entering into cloud computing contracts, such contracts may include transfer of personnel from the business client to the cloud service provider. If this is the case, it should also be kept in mind that the termination of the cloud service contract will revert the transfer of the employment contract to the business client.

TAXATION

Applicable tax rules

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

Professional cloud computing service providers are subject to the standard corporate tax under the French General Tax Code. The standard corporate tax rate is currently set between 28 per cent and 31 per cent depending on the taxable turnover, and will be lowered to 25 per cent for all entities by January 2022. French corporate tax applies to entities exercising an activity in France and other entities of which the taxation is attributed to France according to international tax conventions.

To be considered as exercising an activity in France for tax purposes, the corporation must have a 'fixed establishment' on French territory according to the definition of the Organization for Economic Cooperation and Development (OECD) Model Convention. In the absence of equipment and personnel, a service provider is likely not considered as having a 'fixed establishment' on French territory. The inability to tax digital service providers due to this rule has led the French government to adopt a specific tax only applicable to digital service providers with revenues exceeding €750 million worldwide and €25 million in France. This tax has been temporality suspended in anticipation of an amendment of the notion of a 'fixed establishment' within the OECD model convention and the adoption of tax treaties for cross-border digital services.

Indirect taxes

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 principal indirect tax applicable to cloud services in France is the value added tax (VAT). The standard rate of VAT, 20 per cent, applies to cloud computing services when they are provided in return for payment. According to the French General Tax Code, cloud computing services are considered 'electronically provided services'. Article 98 C of Annex 3

to the General Tax Code explicitly designates 'the provision and hosting of websites, the remote maintenance of computer programs and equipment' as electronically provided services. Owing to the nature of cloud computing services, the determination of the location of taxation, governed by articles 259 et seq of the General Tax Code, can give rise to complications for the application of VAT. According to article 259 D of the General Tax Code, VAT is collected in France if the service is provided by a service provider subject to VAT and located outside the European Community for a client not subject to VAT established or domiciled in France.

RECENT CASES

Notable cases

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.

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

The record fine of €50 million under GDPR imposed by the French Data Protection Authority provides an example of data protection standards applicable to large software-as-a service (Saas) providers offering a wide range of integrated services to end users. The French Data Protection Authority, the CNIL, noted the fragmentation of information documents provider to end users and ruled that Google was in breach of transparency obligations and had not obtained valid consent from users. The breadth and variety of data processing operations, in large part related to Google's various SaaS services, and the large number of persons concerned were invoked as aggravating factors. This decision was appealed by Google LLC before the French Supreme Administrative Court, which upheld the CNIL's decision in a ruling dated 19 June 2020.

UPDATE AND TRENDS

Key developments of the past year

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?

Brexit and the recent invalidation of Privacy Shield by the European Court of Justice present challenges as well as new opportunities for the French cloud market and its actors as cloud services involving personal data may need to be adjusted to accommodate these new developments and ensure compliance with data protection laws.

Tension surrounding the market domination by foreign actors and the emphasis on the need to develop a 'sovereign cloud' is expected to continue, as is shown by administrative lawsuits lodged against government cloud service contracts. The entry into force of the European Electronic Communications Code scheduled for December 2020 and the resulting application of the ePrivacy Directive on over-the-top services adds another layer of complexity to the existing regulatory framework.

Finally, the increasing reliance on remote work and, in consequence, cloud services owing to the covid-19 crisis is also accelerating the adoption of cloud solutions by French entities.

Coronavirus

What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Although no specific legislations or relief programmes regarding cloud computing have been adopted in France, the ongoing covid-19 pandemic and the government policy encouraging remote work to the extent possible has been, and is expected to continue to contribute to the development of the cloud market.

The government also announced the deployment of additional funds of up to €500 million to mitigate the impact of the covid-19 crisis on tech firms.

LAW STATED DATE

Correct on

Give the date on which the information above is accurate.

17 September 2020.