



Access
Partnership

Public Procurement and Cloud Service Providers in France

Summary

The French public procurement system is a complex administrative and political structure, with several levels of contracting and oversight. Despite one central set of rules, responsibility for procurement is dispersed among local authorities, forming a significant barrier to standardisation. In addition, France has the highest number of procurement proceedings per year within the EU.

The government of Emmanuel Macron has embarked on major digital transformation programme: full digitalisation of public proceedings within five years and a massive reduction in the cost of running the state. To achieve this, cloud procurement is essential. However, France's fragmented and data localisation requirements remain major barriers to cloud adoption.

As experts in the field of regulatory policy, Access Partnership has the knowledge and expertise to help guide clients through the cloud procurement landscape. Our public policy specialists have a thorough understanding of the regulatory environment across France, the EU, and its member states, and possess extensive sector-specific knowledge, particularly in finance and health. These attributes allow us to provide our clients with comprehensive solutions to help achieve their goals with minimal fuss.

This report examines the regulations, rules, and procedures surrounding procurement, and more specifically cloud procurement, in France. We provide a snapshot of the laws, regulations, and guidance that may impact cloud uptake and outsourcing in public, financial, and healthcare sectors.

Overview of Public Procurement in France

The two main references for public procurement are [Ordinance 2515-899 of 23 July 2015](#), the global framework for public procurement, and [Implementation Decree 2016-360 of 25 March 2016](#) containing comprehensive rules.

Both the Ordinance and the Decree transpose [wider EU rules](#). Accordingly, the fundamental principles governing public procurement rules — transparency of procedures, non-discrimination of bidders, equal treatment of offers and the saving of public resources — are in line with the European Directives. However, the Ordinance does not apply to contracts which require secrecy, special security measures, or which are matters of national security. The Ordinance covers legal persons covered by public law, government and government public bodies, local public bodies, and public entities governed by public law.

Responsibility for cloud procurement is spread across departments. The Ministry of Economy and Finance has primary responsibility for the conditions governing the public procurement system. The Legal Affairs Department (DAJ) is in charge of analysing regulations, providing support and legal advice to other departments, and collecting data on procurement through the Public Procurement Economic Observatory (OEAP). Finally, the Ministry of Defence and Ministry of Transport, which make relatively heavy use of public procurement, have developed tools to better inform contracting authorities of the main developments in their respective fields.

When the needs of a public purchaser cannot be met with available solutions, they can use specific contracts such as framework agreements, competitions, and partnerships (or administrative contracts). Additionally, innovation partnerships allow for the joint development of custom solutions, with the public purchaser reviewing each stage of development before acquiring the resulting solution.

French Specificities

The division of civil and administrative courts is not common elsewhere in the EU, creating specific implications for France. France also has specific rules for public network operators (water, energy, telecommunications, petroleum, gas, charcoal and postal services, and transport), national defence, security contracts, and research and development contracts.

Legislation differentiates between three types of need: works, supplies (such as purchase and rental) and services. Those categories matter, since some rules differ according to the qualification of the need (also called "object of the market"). For example, the procurement procedures differ based on the amount and the type needed.

There are also several supplemental rules regarding EU procurement directives. For instance, the Decree of 25 March 2016 bans changes in the composition of a consortium during the award process, with a few exceptions. While grounds for exclusion are identical to those set out in Directive 2014/24, the consequences are harsher under French law. Finally, French law sets out specific award rules for contracts below EU thresholds. For example, any public contract whose estimated value is above EUR 90 000 must be published in set publications.

Digitalisation of Public Procurement

France was an early adopter of digital services when it developed an eProcurement portal several years ago. Only recently, however, has there been real progress, and the government addressed the need for more effective processes in 2017 by adopting the [Digital Transformation Plan for Public Procurement 2017-2022](#). This roadmap for the dematerialisation of public procurement describes 19 actions centred around the five axes: control, simplification, interoperability, transparency, and archiving.

[La Place](#), [Boamp](#) and [Achat public](#) are the main public procurement platforms. They allow companies to respond to consultations from the central government, public services and agencies, and the Chambers of Commerce and Industry.

In addition, France has a central purchasing body called the Union for Grouping Procurements ([UGAP](#)) dedicated to the state, public organisms, and local buyers. It is the only generalist public purchasing centre in France, distinguished by its partnership policy and its commitment to public policies (including innovation, SMEs, and sustainable development).

France and Cloud

In 2014, the Cloud Computing Plan made cloud development a top priority for France's re-industrialisation, but the plan's impact was limited. The Directorate-General of Enterprise (DGE) of the Ministry of Economy published a [guide](#) to cloud computing and data centres for local public entities in 2015. The same year, the State Procurement Service (SAE) created and distributed a standard interdepartmental cloud procurement contract to guarantee that each department could order cloud capacity quickly, simply, and cheaply. The efforts for the interdepartmental cloud strategy were led by the inter-ministerial Directorate of Information and Communication Systems (DISIC). The strategy allowed government agencies to outsource non-critical data to an external infrastructure-as-a-service (IaaS) cloud provider (Orange Business Services in this case) and to develop a private cloud for all internal critical data.

Since then, Eurocloud has been [actively promoting](#) cloud computing in France and the initiative was welcomed by Mounir Mahjoubi, the Secretary of State for Digital, in the summer of 2017. However, despite these actions, officials remain uneasy about non-European cloud computing solutions.

Data Protection

The French Data Protection Authority (CNIL) issued [recommendations](#) on compliance with general regulations for cloud services, including:

- Clearly identifying the data and processing operations that will be stored in the cloud
- Identifying the relevant type of cloud services
- Defining the requirements for technical and legal security
- Choosing a service provider that offers sufficient guarantees
- Carrying out risk analysis to identify the security measures essential for the company
- Assessing the level of protection given by the service provider for the data processed

Foreign Companies

The introduction of a local preference criterion in a public procurement process is prohibited by the European Union. Indeed, the European Court of Justice held that the Treaty prohibits not only overt discrimination of nationality but also all covert forms of discrimination which, by the application of other criteria of differentiation, lead to the same result.

However, the French Administrative Supreme Court ("Conseil d'Etat") ruled that an obligation to establish a local subsidiary may nevertheless constitute a condition for its award, as long as it is justified by the object of the contract or its execution conditions. A candidate that commits to creating a subsidiary if they're awarded the contract meets this requirement.

Data Localisation

Data localisation requirements exist in several areas, including the French Heritage Code, which requires public archive storage infrastructure to be available for inspection, and the NF 461 certification, which only sanctions electronic filing systems that exclude applicants that don't allow precise knowledge of and control over the location of archived documents.

The documents and data produced by public and private persons in the course of a public service are considered part of the public archives and are thus classified as national treasures.¹ This requirement imposes strict localisation rules, since a national treasure may only leave French territory temporarily, after authorisation from the Ministry of Culture, and only for "purposes of restoration, expertise, participation in a cultural event or deposit in a public collection." Additionally, Article R212-23 limits public archives on digital platforms hosted and processed to national territory.²

The Directorate-General for Enterprise (DGE), part of the Ministry of Economy, issued a 2015 guide to cloud computing and data centres for local authorities. The letter suggests that the Ministry "strongly supports the development of a French and European cloud computing industry to answer the issues of sovereignty and access to innovation". It recommends that local authorities select a provider with strict security and confidentiality standards. Similarly, a note published in April 2016 by the Ministry of the Interior and the Ministry of Culture dictates that the use of a non-sovereign cloud is illegal for any institution producing public archives.

The current government is aware of this narrow interpretation and will remove the data localisation requirements for data subject to EU law. This would allow the data centre to be based elsewhere in the EU.

¹ As per Article L111-1 of the French Heritage Code.

² Article [R212-23](#) of the French Heritage Code.

SecNumCloud Label

SecNumCloud, a label from the national security agency (ANSSI), replaces Secure Cloud, which was launched experimentally in September 2014. It is largely based on the ISO 27001 standard and covers all cloud services. The agency also requires data hosting in Europe, as well as first-level support and online customer service in French. These core requirements have been designed based on France and Germany's experience with the certification and qualification of security products and services. For the SecuNumCloud Advanced repository, data centres must be located in France (as will multi-factor authentication and hardware encryption via hardware security module (HSM)). Early in March, Amazon [applied](#) to obtain the label.

Regulatory Landscape for Cloud in Financial Services

There is no specific regulation for IT and cloud services, but the outsourcing of financial services is subject to the Monetary and Financial Code, the French Prudential Control Authority, and the Financial Markets Authority. The entities under regulation are credit institutions, investment firms, legal persons composed of either credit institutions or investment firms and payment institutions.

In the [decree of 3 November 2014](#) "relating to the internal control of companies in the banking, payment services and investment services sector subject to the control of the Prudential Supervisory and Resolution Authority (completing the transposition of Directive 2013/36 / EU of 26 June 2013, Capital Requirements Directive CRD IV". Outsourced activities are defined as those "for which the reporting enterprise entrusts to a third party, on a long-term and customary basis, the provision of services or other essential or important operational tasks". Comparatively, banking and related operations are defined as essential and important business tasks. The outsourcing of all or part of the information systems supporting bank operations is therefore clearly part of the Directive.

A number of requirements must be included in the specifications for outsourcing these information systems:

- the existence of a control system for outsourced activities;
- the ability to identify and manage the risks associated with outsourcing;
- the conclusion of a written contract between the client and the service provider;
- the possibility for the customer to expressly accept any substantial modification of the service;
- the customer's ability to act in case of system malfunction;
- the ability to ensure continuity of business and the existence of a contingency plan;
- the existence of a commitment by the service provider on the level of quality of the service;
- the ability to protect confidential information; and
- the ability to audit on-site services and to provide access to information by the prudential supervisor.

As public entities, the French Central Bank, Financial Market Authority (AMF) and the Prudential Supervision and Resolution Authority (ACPR) are subject to EU Directive 2014/24/EU, Ordinance n° 2015-899 of July 23 2015, and Decree 2016-360 of the 25 March 2016.³ Depending on the value and nature of the contracts, the AMF and ACPR will publish calls for tender in the Official Bulletin of Government Procurement (*Bulletin Officiel des Marchés Publics*), the Official Journal of the European Union, and on achatpublic.com.

The French financial authorities participated in the development of European reports and comply with guidance from national agencies (like the ANSSI) as well as European guidance (the EBF and EBA). Additionally, the French Banking Federation ([FBF](#)) released several reports on cybersecurity and the digitalisation of banking, which significantly contributed to the development of the "Digital Vision Paper" led by the European Banking Federation (EBF). This document presents proposals for the realisation of the Digital Single Market, covering electronic identity (e-ID), data, cloud, cybersecurity, and payments.

In July 2013, the ACPR published [a report](#) on the risks associated with cloud computing, and the AMF and ACPR recently signed a partnership with the ANSSI for enhanced cooperation in the field of information system protection. This includes regular exchange of information between financial regulators and the agency concerning incidents affecting the security of information systems.

Regulatory Landscape for Cloud in the Healthcare Sector

The health sector has developed specific certification procedures for service providers.

L'Agence Française de la Santé Numérique ([ASIP Sante](#)) is the French agency for digital health. Its main tasks are to create the conditions for the rise of e-health, lead national projects, and deploy and support innovation. The Agency has published several guidelines regarding digitalisation and data management in the health sector, including a "[Global Information Security Policy for the healthcare sector](#)", as well as defining a reference framework for the constitution of accreditation application files hosting personal health data.

The Ministry of Health is responsible for the pre-appraisal of applications and the secretariat of the accreditation committee. As such, it plays a central role in ensuring that French and EU rules are implemented, as well as observing and measuring changes in the hosting of health data and measures to evolve the process.

[COFRAC](#) is responsible for all accreditation programs that require a specific approach regarding human health. The certification procedure is based on a conformity assessment in which the host chooses a certifying body that must be accredited by COFRAC (or equivalent at European level). The organisation carries out a two-step audit to assess the host's compliance with the requirements of the certification framework.

³ Note that the Ordinance does not apply to Financial services contracts relating to the issue, purchase, sale and transfer of securities or other financial instruments, in particular the supply of money or capital by contracting authorities or contracting entities. It does not apply to Financial services markets, except insurance services.

The French health sector also has a central purchasing body called [RESAH](#), active on behalf of 150 member hospitals and nursing homes.

France – Key Takeaways

- France is one of the most digitally conservative member states in the EU.
- The most critical obstacle to widespread cloud adoption and optimal use remains the decentralised nature of IT in the French government, which makes it virtually impossible to get all agencies moving in the same direction.
- While adoption of private cloud computing is in line with other countries, the French government's adoption of public cloud lags far behind.
- Security and national sovereignty considerations are major obstacles to moving public sector data and applications to the cloud. There is an ongoing debate between the current government and various ministerial departments.



Access Partnership

www.accesspartnership.com



[AccessAlerts](#)



[AccessPartnership](#)



9th Floor, Southside
105 Victoria Street
London SW1E 6QT

