CCN-CERT

BP/31

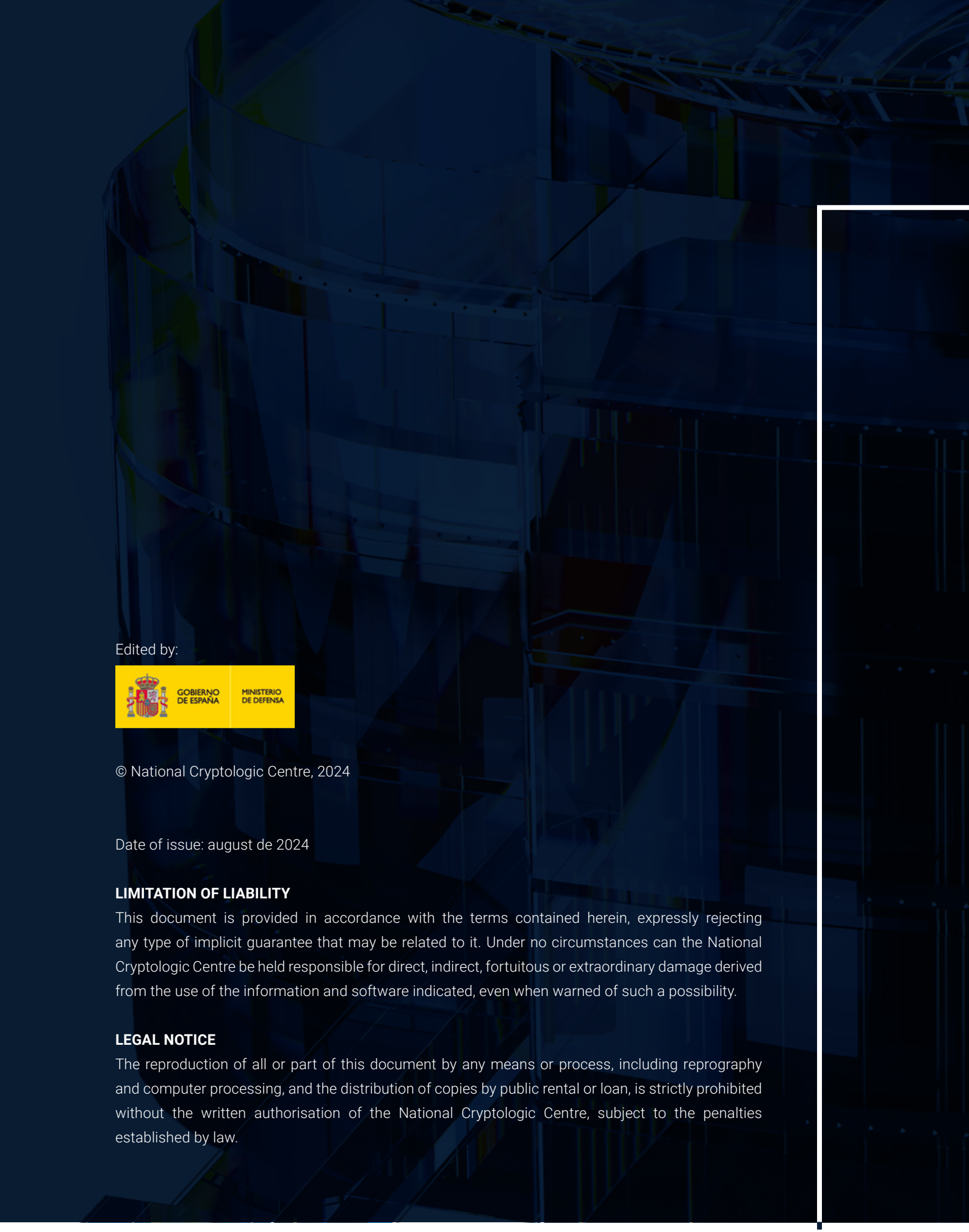
Data Protection in the Cloud: Digital Sovereignty

BEST PRACTICES REPORT

MAY 2024

ccn-cert centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional



Edited by:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Date of issue: august de 2024

Index

1. Purpose of this document

This guide aims to provide an updated overview, together with some recommendations, of the technological solutions and resources typically offered by Cloud Service Providers (CSPs), as well as to review the state of the art of hyperscale providers' technology and solutions to ensure digital sovereignty, including aspects related to data confidentiality, integrity and availability.

To this end, the guide describes the different technical, organisational and contractual measures that CSPs must comply with in order to mitigate the risk scenarios associated with this type of solutions. The risks described cover different scenarios related to logical and physical security, privacy, as well as certain regulatory aspects applicable in the European Union.

Without being an exhaustive guide, it is intended as a reference document so that technical and business leaders can find the necessary balance to innovate and, at the same time, comply with security requirements in the Cloud. This Guide should be consulted in a complementary manner to the guides published by the National Cryptologic Centre, in particular CCN-STIC-823 (Use of Cloud Services).

2. Introduction

The ISO/IEC 19941:2017[1] defines Cloud computing as the paradigm that enables network access to a scalable and elastic pool of shareable physical resources, or virtual resources with self-service provisioning and on-demand management. Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

The cloud service provider must have a robust and secure infrastructure, one or several independent and physically separated data centres in different areas, with sufficiently oversized equipment (hyperscale), and from which it can offer instances to its users individually, automatically creating technological resources of all kinds through code, with virtually no limitations, neither in number nor in capacities (Computing, Artificial Intelligence, security solutions, Satellite and 5G Communications, massive data analysis, storage in a multitude of formats, databases, telecommunications networks, etc.). In any case, the use of the Cloud introduces new architectures and security paradigms that need to be properly contemplated.

The provision of cloud technologies is a model that allows network access, securely and on demand, to a set of configurable technological resources. These resources can be supplied and deployed quickly, allowing self-management and self-service, thanks to the automation of service management. Spanish Public Administrations are increasingly benefiting from this new technological paradigm, although it requires adequate training and knowledge to understand which Cloud security model is ideal for each need.

1. https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en

2. Introduction

In short, the aim is for cloud services to be supported by architectures that, on the one hand, offer the necessary security, compliance with legislation, protection and data sovereignty and, on the other hand, have the necessary functionalities to support the business strategy in order to innovate and reduce time-to-market. Once this balance between security, compliance, objectives, business growth and innovation or digital transformation is achieved, the user is offered the flexibility, agility, scalability and cost of choice according to their needs, in addition to offering the public cloud the advantage of helping organisations to advance their sustainability objectives.

It is precisely this multiplicity of options that obliges those who intend to benefit from Cloud services to carefully study the different offers on the market, together with their own business requirements, their corresponding risk analysis in order to be able to select the appropriate solution and safeguards that best suit their risk appetite, while safeguarding compliance with the provisions of the legislation in force.

3. Basics of Cloud technologies[2]

The Cloud technology model allows on-demand access, from any physical location with Internet access, to a set of configurable computing resources (e.g. networks, servers, storage, applications and services in general) that can be requested and released immediately, with minimal management effort.

3.1 Definition of public, private and hybrid Cloud

3.1.1 Public cloud

A public cloud is a cloud computing model in which IT infrastructure such as servers, networks and storage resources are provided as virtual resources accessible via the Internet.

Traditionally, organisations had to acquire and self-manage the infrastructure needed to run applications. It was costly to set up and maintain, and advanced computing capabilities remained out of reach for many organisations. The public cloud solved these challenges by making IT resources accessible as fully managed services.

2. See CCN-STIC 823 ICT Security Guide

Thus, an external provider maintains the hardware, relevant software and licences in a territorially distributed network of data centres. The user organisation can access only what it needs on demand and at any scale from any device it chooses. Your organisation can use the public cloud to access cutting-edge and emerging technologies, such as artificial intelligence (AI) services, distributed logging technologies or the internet of things (IoT), increasing the speed and adoption of technological advances and helping to improve service delivery and customer satisfaction.

3.1.2 Private Cloud

A private cloud is one in which the necessary infrastructure is dedicated to a specific customer or tenant, i.e. no resources are shared with third parties, regardless of whether that underlying infrastructure for providing resources is owned, managed and maintained by the organisation itself (on-premise), or outsourced to a CSP.

The term *private cloud* was introduced to establish a distinction between these cloud environments on an infrastructure under the sole control of the organisation (whether internal or external dedicated) and public cloud services provided by external providers on a shared (multi-tenant) infrastructure.

3.1.3 Hybrid Cloud

A hybrid cloud is a configuration in which an organisation uses both public and private Cloud. It hosts an IT infrastructure design that integrates dedicated IT resources (usually internal to the organisation) with infrastructure and services from Cloud providers. With a hybrid Cloud, data can be stored and applications can run in several distinct environments.

Organisations often adopt hybrid Cloud strategies to overcome the limitations of the private Cloud, allowing them to continue using their existing on-premises data centre, accessing the public Cloud as needed. Likewise, hybrid Cloud allows you to seamlessly alter workloads between different environments. When organisations run out of computing resources in the internal data centre, they extend capabilities by shifting the extra workload to external, third-party Cloud services. *Scaling in the Cloud* is an appropriate and cost-effective way to support workloads that have varying demand patterns or seasonal peaks in demand.

3.2 Essential features of the Cloud

3.2.1 Self-service on demand

In this mode, and from a control panel, the cloud service customer can unilaterally manage the provision of cloud resources as needed, such as computing power, storage space, database capacity, all without requiring any human intervention by the provider, always within the parameters of the contracted licence of use.

It is common for the configuration of services to be carried out through a conventional browser, accessing a web control panel, where the administrator can carry out all the necessary operations to request Cloud services and manage them. This feature allows any Cloud operation to be carried out via an API call, which enables a high degree of automation and monitoring of all Cloud requests.

3.2.2 Pay-as-you-go

Under this modality, the customer consuming a cloud service only pays for the individual services he or she needs for as long as he or she uses them, without the need to enter long-term contracts or complex licences. They are said to be similar to the concept of water and electricity tariffs because you only pay for what you consume and once the service is cancelled, no additional costs or cancellation fees apply.

3.2.3 Cost reduction

Another characteristic of the Cloud is the reduction in costs compared to traditional computing. This is mainly due to the innovation and automation involved in the use of cloud technologies and infrastructure. Economies of scale in those hyperscalar providers lead to lower and more competitive prices. Innovation in hardware, such as CPUs, network cards and other components, as well as the automation offered by cloud services, constantly reduce the prices offered to the customer.

3.2.4 Global access

The services are available on the Internet and are accessed through standard mechanisms that allow the use of thin clients, such as mobile phones, tablets, laptops and workstations, and do not require any specialised software installation to manage them.

This allows any type of device to be a means of accessing this environment for both management and use.

3.2.5 Set of dedicated or shared resources for a client

As noted above, the resources where compute instances are running can be dedicated to one customer or shared among several of them; for example, a data centre within a certain supranational union (such as the EU), or state (such as Spain), dedicated exclusively for certain specific customers, or for a set of specific customers belonging, for example, to a government or an institution. The specific customer could be running loads in the private, public or hybrid Cloud.

In the case of the private cloud, instances would be shared only between the same type of customers.

In the case of the public Cloud there are two possibilities:

- Where a client runs virtualised instances on the same server and shared among other clients, and where software and hardware resources rely on logical isolation mechanisms to protect their data.
- Where some public cloud providers offer dedicated server instances (without virtualisation) where the customer can run an instance on the server, with or without virtualisation, completely isolated from other customers, thus avoiding logical isolation of hardware and software and increasing data protection.

Adoption of either model may come at the cost of sacrificing access to more advanced cloud technologies, as this is typically the case in the IaaS model. As a general rule, cloud providers continuously publish and update their technological innovations so that they are immediately available. The private or restricted Cloud option implies giving up access to technologies available in the public Cloud used by a growing majority of organisations in various sectors.

3.2.6 Elasticity and scalability

The Cloud provider's computing resources enable on-demand services to be provided to multiple client organisations; physical and virtual resources that are dynamically allocated, de-allocated and re-allocated according to the demand of the users of the services, enabling contracted capacities to be elastically increased or decreased, in some cases automatically, to rapidly scale contracted services according to the demand users have for them.

Thus, from the perspective of the cloud services customer, the available resource capacities may appear to be unlimited and can be provisioned in any quantity and at any time, always within the contractual and billing agreements of the service consumed.

All of this means, in short, that the resources required are scalable, i.e., it is possible to initially contract a certain service quota and grow progressively, depending on the demand required, according to the client's needs, with total immediacy, without having to maintain human interaction between provider and client, thanks to the high degree of automation of the processes and systems offered by the cloud provider.

3.2.7 Innovation and digital acceleration

The Cloud offers innovation to the customer through continuous R&D and competition between Cloud providers, who are constantly developing new services and technology and improving their efficiency, enabling the customer to benefit directly, reducing their time-to-market and quickly turning their ideas into opportunities to accelerate their digital development.

3.2.8 Resilience

The use of the Cloud allows for increased IT resilience, observable from both sides of the shared responsibility. On the one hand, the provider offers an infrastructure consisting of redundant facilities and networks (hardware and software), which enables disaster recovery and availability up to a contractually agreed SLA level. On the other hand, the customer has to know how to use this infrastructure to configure its cloud-deployed solutions to meet its resilience requirements. The degree of automation of cloud providers often offers greater resilience than a traditional data centre.

3.2.9 Security

Strong security is crucial to underpin digital transformation and innovation. Cloud service providers offer help to organisations to develop and turn security, identity and compliance into key business enablers. Cloud providers make security a top priority, designing more secure cloud infrastructures, automating security to create an environment that drives the speed and agility required by their customers, relying on vendor partners and a broad portfolio of security solutions. Several IDC and Gartner[3] reports point out that security in the Cloud is stronger than in a traditional data centre, something that can be demonstrated by the multiple national and international security standards and certifications that public Cloud providers obtain and maintain.

3.2.10 Monitoring of the service

As we have pointed out, cloud computing services can be managed automatically, optimising their use through automated monitoring and management, enabling efficient use of the infrastructure. However, the use of resources can also be queried, monitored and controlled by the customer, providing greater transparency for both the provider and the consumer of the service used.

3. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Monitoring allows, as a derivative feature, pay-per-use of the services contracted in the Cloud, allowing easy adaptation to the changing needs of the organisation without committing excessive budgets, and improving responsiveness to changes that may occur.

3.2.11 Sustainability

Sustainability, understood as the ability to meet the needs of the present without compromising one's own or collective needs for the future, is a crucial goal for society. Its benefits include a healthier planet, better conserved natural resources and a more resilient economy.

In this context, moving workloads to the Cloud can be a strategic decision for companies seeking to contribute to sustainability. The Cloud offers a number of advantages that translate into a lower environmental impact:

- **Energy efficiency:** Cloud data centres are designed to optimise energy consumption, using state-of-the-art technologies and renewable energy sources.
- **Waste reduction:** The cloud eliminates the need to purchase and maintain proprietary hardware, which reduces the amount of e-waste generated.
- **Scalability:** The cloud makes it possible to adjust computing resources to real demand, avoiding unnecessary energy consumption.
- **Flexibility:** The cloud facilitates the adoption of sustainable practices, such as auto-shutting down servers at off-peak times or scaling up when needed.

Ultimately, moving workloads to the Cloud not only benefits businesses in terms of cost and efficiency, but also allows them to contribute to a more sustainable future.

3.3 Cloud computing service models

The different service models are linked to the role of the cloud service provider regarding the different layers that make up the solution, such as network, storage, physical servers, virtualisation, virtual machine operating systems, middleware, applications and data.

Customers of Cloud services can decide up to which level or layer they decide to delegate the required services to the provider. A simplified picture is shown below that does not take into account concepts such as encryption by the CSP and/or the CSC, nor the upper layer consisting of the data itself brought to the Cloud.

Three (3) basic Cloud service models are considered:

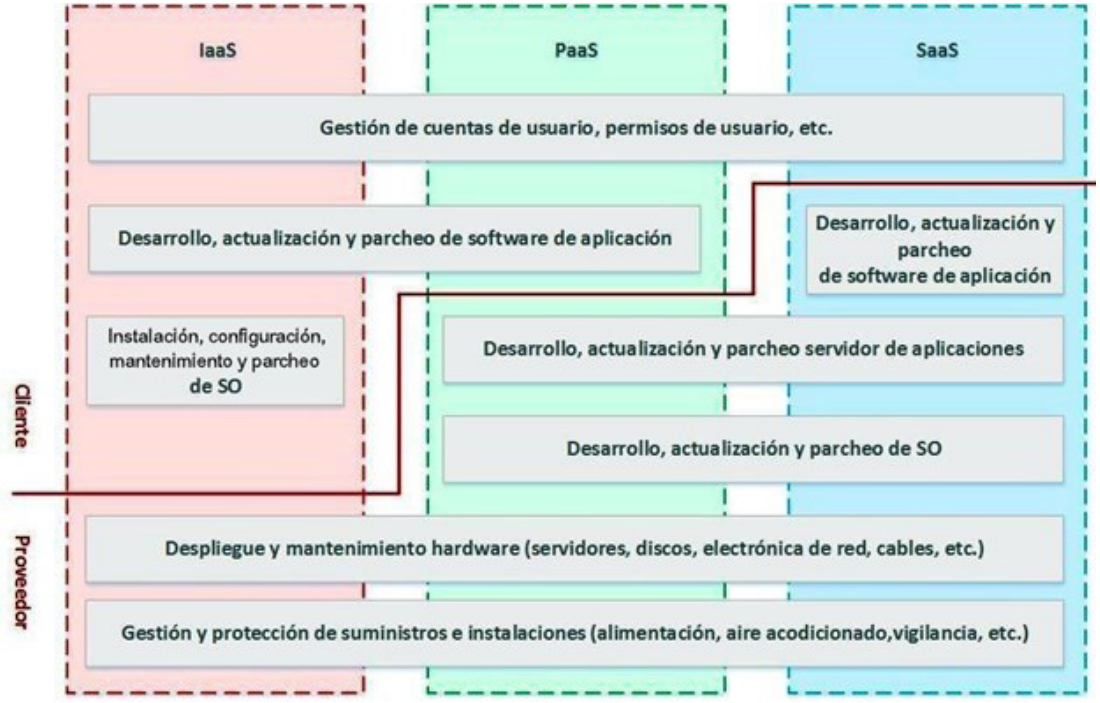


Figure 1.- Responsibility in each of the service models

3.3.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service, sometimes abbreviated IaaS, contains the fundamental building blocks for cloud IT. It typically provides access to networking features, hardware (virtual or dedicated software) and data storage space. Infrastructure as a Service offers the highest level of flexibility and management control around IT resources and bears the closest resemblance to the existing IT resources with which many IT departments and developers are familiar but does not maximise the potential savings that could be made by reducing the required operation of the infrastructure by transferring it to a third party.

This cloud computing service model in the case of IaaS consists of contracting one or several virtual, shared or dedicated servers, at most including the operating system. On these servers, the client will host its applications and/or databases in the contracted space.

In this model, the cloud service provider is limited to maintaining the hardware and supplies and supervising that the virtual servers function correctly from the point of view of service availability; without access to the content of the information hosted on the server instance. The client has mechanisms for uploading and downloading data and applications in a totally autonomous and secure manner.

3.3.2 Platform as a Service (PaaS)

In this model, Platform-as-a-Service eliminates the need for companies to manage the underlying infrastructure (typically hardware and operating systems) and allows them to focus on deploying and managing their applications. This helps improve their efficiency, as they do not have to worry about resource provisioning, capacity planning, software maintenance, patching, or any of the other tasks involved in running their application.

In this model it is exactly the same as in IaaS: the provider merely manages the full functionality of the underlying services without access to the customer's data.

3.3.3 Software as a Service (SaaS)

In this model, software as a service provides a complete product that the service provider runs and manages. In most cases, those who talk about software as a service actually mean end-user applications. With SaaS, you don't have to think about how the service is maintained or how the underlying infrastructure is managed. The customer of the service only has to worry about how to use that particular software system.

A common example of a *SaaS* application is a web-based email programme that allows you to send and receive messages without having to manage the addition of features or maintain the servers and operating systems on which the email programme runs. The customer will have to pay a rental or licensing fee and is solely responsible for properly configuring the application to implement the configuration and operational controls necessary for the protection of its data.

In this model, the SaaS service provider may not have its own infrastructure and may have to outsource it to an IaaS or PaaS service provider, whereby the so-called outsourcing or supply chain regime may come into play.

In this model it is exactly the same as in IaaS: the provider merely manages the full functionality of the underlying services without access to the customer's data by the SaaS provider.

3.4 Shared responsibility according to the type of service used

We can speak of security "from" the cloud and security "in" the cloud, depending on the chosen service model. Figure 1 shows that there is a balance of responsibility between customer and provider.

Cloud Security. The CSP shall be responsible for the maintenance and security of the services it provides to the customer, as well as for complying with any service level agreements and contractual agreements that may be established. It shall cover the security of the hardware, software, networks and facilities that operate the Cloud services, as well as compliance with the legal regulations applicable to this type of services.

Cloud security. The customer's responsibility shall be limited to the operation, management, configuration and security of the services deployed on the Cloud that are not owned by the CSP (for example, a virtualised operating system in the IaaS model), as well as the configurations established, based on the functionalities offered by the provider depending on the type of service and the Cloud service model (IaaS, PaaS, SaaS) contracted, in addition to the responsibility for the legal compliance of the services deployed on the Cloud.

3.5 Cloud computing deployment models

Three (3) cloud computing deployment models are considered, with possible variants on some of them.

3.5.1 Private Cloud Deployment

The private Cloud is the one created by the organisation itself to host its information through virtual servers and self-provisioning and orchestration functionalities, accessed through the Internet.

This deployment model is therefore the one that differs the least from the classic data processing centre solutions resident in the user organisations. This alternative forgoes most of the advantages offered by the cloud. It incurs high fixed costs, regardless of how the cloud is used, while making it more difficult to comply with the optimisation of energy use and the use of renewable energies, which are more typical of the public cloud.

3.5.2 Deployment as Public Cloud

The public cloud is where a cloud service provider makes its platforms and infrastructure available to the market for its different customers to host their data. The hardware and software infrastructure, depending on the service model chosen, is shared between the different customers (multi-tenant) or dedicated separately between them (single-tenant).

In other words, single-tenant and multi-tenant are two models of deployment of cloud solutions by providers. The main difference is that single-tenant offers one server instance that is not shared with other customers, while multi-tenant allows a server to be shared between different customers, but within the server, several individual and secure software instances are created and managed by each customer.

The multi-tenant model is considered to be more scalable, efficient and cost-effective than the single-tenant model, but offers a larger exposure area, so CSPs must adopt more robust security measures than in a single-tenant model.

NOTE: Some authors consider the 'single tenant' as a particular case of private Cloud, instead of considering it as one of public Cloud, restricting the latter to what is known as 'multi-tenant'. This conception has been used in the definitions section 3.3 of this guide.

3.5.3 Deployment as a Hybrid Cloud

Hybrid Cloud is a mix of both private and public, depending on the applications, the nature of certain data to be handled and the context of the organisation. Hybrid Cloud deployments may also include legacy infrastructure on-premises.

For a deployment to be considered a hybrid Cloud, the different Cloud environments must be tightly interconnected with each other, operating as a combined infrastructure.

4. Digital sovereignty and its requirements

4.1 Definition of digital sovereignty

The concept of digital sovereignty varies in its definition, but in essence it seeks to indicate that the data is subject to the laws and governance structures of the country and organisation that owns the data[4]. It focuses on control over the data, its location and access, the infrastructure, software and regulatory compliance necessary to create and operate the digital world[5]. However, digital sovereignty also encompasses other aspects such as digital transformation, resilience, innovation and competitiveness, as well as having a strong geopolitical component.

The approach to digital sovereignty compliance depends on a number of factors that regulators, businesses and providers need to consider. On the one hand, there are the inherent security and privacy risks, and on the other hand, there is the competitive advantage that technologies such as the cloud offer businesses to help them innovate and compete in a free, digital and global marketplace.

This section describes what the different digital sovereignty requirements are, and then describes technical, organisational and contractual measures to meet these requirements offered by each provider under consideration. This provides the reader of this guide with the different options and measures they can use around digital sovereignty.

---

4. https://d1.awsstatic.com/whitepapers/Whitepaper_Overcoming_the_Tension_Between_Data_Sovereignty_and_Accelerated_Digital_Transformation_2022.pdf

5. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

4.2 Digital sovereignty requirements

The user of this guide should analyse and assess what technical, organisational, contractual and regulatory measures are necessary to comply with these requirements, considering the cost/benefit, business objectives and the policies and regulations that the organisation has to comply with.

Both the user and the cloud provider are subject to current legislation which, depending on the classification of data required by the cloud user (personal, sensitive or classified data), must be complied with (General Data Protection Regulation, National Security Framework or Official Secrets Act, among others). In practice, their application may be required as a combination of several of the aforementioned legal standards. Additionally, there are also other legislations that apply, such as Law 40/2015, of 1 October, on the Legal Regime of the Public Sector and Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations. The legislation in force or, where applicable, the contractual clauses contemplate the following requirements that are detailed in the following sections of this chapter:

- **Territoriality of the data and possible international transfers:** this will reflect the territoriality of the Data Centres (DPC) where the information of the customer contracting cloud services will be located.
- **Jurisdiction to which the parties are subject to the contract:** the contract should reflect to which law the processing of data in relation to the customer will be subject, outlining as many identifying details of each organisation as possible so that the customer is not helpless when seeking to assert his or her rights.
- **Limitation of liability:** these are the respective contractual obligations of each party (CSP and customer) and should be protected from those that represent a significant risk to them.
- **Transfer of control or data portability:** this clause provides for a situation of change of control in the CSP where, upon such changes, the customer has the right to port his data to another CSP.
- **Service level:** represents the understanding between the customer and the CSP about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the specified level, sets the compensation for the customer.

- **Termination clause:** protects the customer against the CSP, in case of a serious degradation or breach of the expected and contracted service level (SLA/SLA).
- **Confidentiality:** the CSP's obligations regarding confidentiality, i.e. that the CSP will not disclose its customers' data to unauthorised third parties, must be covered.
- **Intellectual property:** refers to the due protection of intellectual or industrial property rights, copyrights, patents, trademarks and industrial design.
- **Supply chain compliance:** the CSP must comply in a transparent manner, providing sufficient guarantees regarding technical, organisational and contractual data security measures throughout the supply chain, in accordance with applicable legislation and contracts.
- **Incident reporting:** this clause should clearly define the mechanisms for reporting incidents, especially security incidents, between the CSP and the customer.
- **Early termination:** this clause refers to early termination of the service by the customer, either due to breach of the SLAs/SLAs by the CSP, or due to any other circumstance, such as having found a better offer.

NOTE: All of these clauses are discussed in depth in the annex at the end of this guide.

4.3 Royal Decree 311/2022 of 3rd May

The National Cryptologic Centre (CCN), developing the provisions of Royal Decree 311/2022 of 3rd May, which regulates the National Security Framework (ENS), has established a strategy based on shared responsibility and the joint definition of security mechanisms in cloud environments.

Both the supplier and the customer need to carry out a prior risk analysis to help mitigate all risks, not forgetting the contractual agreements including the clauses or requirements described in section 4.2 of this guide. In this sense, the ENS serves as a basis to help establish a strategy and a control framework based on the creation of Specific Compliance Profiles (SCPs) for security, which allow for the transfer of confidence to organisations, whether they belong to the public or private sector, in the scope of application of the ENS.

Figure 2.- Cloud security strategy

4.3.1 Requirement to comply with the ENS

Compliance with minimum security levels must be established and certified in accordance with the provisions of the ENS. In the case of taking information to the Cloud with some type of restriction in its handling due to its sensitivity or classification, a Certificate of Compliance with the ENS of category HIGH of the system owned by the CSP where the services offered are hosted or, if it exists, a Specific Compliance Profile for a specific solution in the Cloud must be required, all in accordance with the mandatory prior risk analysis that the entity responsible for the processing of the data must perform.

Solutions that are deployed in the cloud require some considerations when contracting and using cloud services. These considerations, dealt with from the ENS perspective, will be included in the *CCN-STIC guide 823 Use of Cloud Services*, as well as in other more specific CCN-STIC guides oriented to solutions.

The risk analysis performed should consider the use of software or hardware security components in the environment, and whether or not there is a need for any formal approval or certification of these components.

4.3.2 Specific Compliance Profile (SCP)

By means of the Certification of Conformity with the ENS in the HIGH category, the security baselines in the use of cloud services will be assured. However, the wide possibilities of customisation and configuration that cloud services can provide may limit the CSP's ability to implement security measures, and in some cases it cannot be held responsible for the configuration defined by the cloud service customer (CSC).

Within the Supplier Relationship Management (SRM) oriented CSC and CSP, it is worth noting:

- **The CSP** is aware of the security commitments it makes to the CSC on the basis of the ENS Conformity Certification it holds, of its category and of the services included in the scope, and always in accordance with the security requirements expressed by the client.

- **The CSC** chooses certain services of a CSP on the basis of its risk profile, but it is not enough to choose the CSP/Contracted Services binomial, it must also follow the secure configuration guidelines, also designated as basing guidelines, provided by the CSPs for some of their services, whether these are the Guidelines published by the CCN or directly by the CSP itself, if the former does not exist.

This responsibility of both parties, the commitments adopted by the CSP on the basis of its ENS Compliance Certification and the actions that the CSC must carry out to ensure the security of the contracted services within its configuration possibilities, may be included in a **Specific Compliance Profile, validated by the CCN**, and its associated security configuration guides, where it is established which security aspects will be the responsibility of the CSP and which will correspond to or be parameterisable by the CSC.

Along with the adoption of such a Specific Compliance Profile (SCP), an analysis of the main risks to which the system is subject, as well as the security measures necessary for their mitigation, should be carried out.

The ECP shall contain a Statement of Applicability detailing the list of security measures that shall be applicable and the responsibility of the CSC, accompanied by the necessary secure Configuration Guidelines so that the CSC can implement those security configurations required in the cloud service whose implementation is the responsibility of the CSC itself.

As mentioned above, this ECP must be validated by the National Cryptologic Centre to ensure that the security standards set out in the ENS are safeguarded, and will be published as a validated Specific Compliance Profile for certain solutions or services offered by the CSPs to which it applies.

4.3.3 Monitoring mechanisms

In addition to the publication of the Specific Compliance Profile (SCP), the cloud service shall have mechanisms in place to monitor the status of and compliance with the security measures set out in the Statement of Applicability.

This ECP, together with the defined security configurations, and having implemented the monitoring mechanisms provided by the CSP, should enable the replication of a security scenario that ensures the storage and processing of sensitive or classified information in the cloud in a secure manner.

It is important to understand that a CSP usually has a wide range of client organisations with different security requirements, with solutions adapted to the needs of all of them. The Catalogue of ICT Security Products and Services published by the CCN, or the appropriate application of specific ENS measures (such as [op.nub], for example), or the observance of the CCN-STIC Guidelines, contemplate the security measures that are considered most appropriate.

Obviously, any modification of the security measures adopted by the CSP that has an impact on the related ECP will first be validated by the CCN, prior to its commercial exploitation in the ENS domain.

4.3.4 Secure Cloud scenarios

The set of instructions (e.g. guidelines, procedures or source code) necessary for the implementation of any cloud security scenario, as well as any mechanism enabling automated replication of a cloud scenario, shall be validated by the CCN and, where appropriate, published together with the ECP.

In addition, and given the rapid evolution of threats affecting information systems, the CSP must have the capacity to adapt to any scenario that presents a security risk throughout the life of the cloud service, guaranteeing the implementation of security measures in accordance with current legislation.

In those aspects of safety where, in accordance with the prescriptive risk analysis, a CSP has identified from a given moment serious security risks in the service that cannot be mitigated by implementing the security measures included in the PCE to which it subscribes, compensatory measures must be implemented to mitigate the new risks effectively, and the CCN must be notified of these measures in order to be able to adapt the PCE if necessary.

4.3.5 Support solutions from the National Cryptologic Centre

A good practice complementary to everything provided by CSPs in the interest of Digital Sovereignty of their Cloud Computing clients is, for example, to implement data protection solutions on its own, such as the CCN's CARLA solution. CARLA is a tool aimed at data protection and traceability, regardless of where the data is located, whether in local mode or in the Cloud.

For each document, or set of documents, the organisation that is client of cloud services defines who has the right to access it in clear. As all documents are transparently labelled (as long as a named agent and the corresponding authorisation are available, the document can be accessed directly), once the access permission has been withdrawn by the organisation that owns the document, the document cannot be decrypted and, consequently, cannot be accessed regardless of where it is located. Consequently, documents cannot be read by third parties in the event of a hypothetical security breach with data leakage.

4.4 Applicable information security legislation

In Spain, affecting the public sector and the private sector that provides solutions or services to it, we have at least two (2) legal regulations that determine, among other aspects, the security measures to be applied to the information systems that support the services and the information handled by them, depending on certain circumstances:

4.4.1 Official Secrets Act (LSO)

4.4.1.1 Introduction to LSO

The importance of the protection of classified information (CI), for those organisations that keep it or process it in their information systems, is regulated by Law 9/1968, of 5 April, on official secrets (LSO), modified by Law 48/1978, of 7 October and developed by Decree 242/1969, of 20 February.

Classified information is also addressed in the National Security Strategy, which recognises that this information is a prime target for hostile intelligence services, for terrorist groups aiming to threaten our security and destabilise our democratic system, and for other countries with economic or commercial interests in competition with those of our industry.

In Spain, *classified matters* (the name adopted by the Spanish Organic Law on Offences against the Official Secrets Act) may be classified as SECRET and RESTRICTED, and there are also *matters of internal secrecy*, which may be classified as CONFIDENTIAL and LIMITED DISCLOSURE.

4.4.1.2 Cloud outsourcing criteria

In the first instance, we will distinguish two (2) different possibilities based on the extent of the information we intend to outsource to a CSP:

- Systems that handle classified information (SECRET, RESTRICTED or CONFIDENTIAL). Using the *CCN-STIC-301 ICT Security Measures to be Implemented in Classified Systems* as a reference.

Systems handling LIMITED DISCLOSURE (LD) information that could be initially equated in terms of the security measures required, in the absence of the mandatory risk analysis, with systems handling sensitive ENS information in the HIGH category.

If we combine these two (2) possibilities with the existing Cloud Computing deployment models, we get up to four (4) different scenarios:

Scenario nº 1 - System handling CI of higher grade than LD and private Cloud: if the private Cloud is owned by the client organisation and not shared with third-party organisations (single-tenant), even if it is not equivalent to developing with own infrastructure in a Restricted Access Area (RAA) of the contracting organisation, such outsourcing could be considered appropriate with contractual safeguards and accreditation of the RAZ of the contracted CSP.

Scenario 2 - System handling LD-grade CI and private cloud: if the private Cloud is owned by the client organisation and not shared with third party organisations (single-tenant), even if it is not equivalent to developing with its own infrastructure in a secure area of the contracting Agency, this outsourcing could be considered appropriate with contractual safeguards and accreditation of the awardee establishment or, failing this, by providing the ENS certification in the HIGH category of the secure area containing the private infrastructure and data, since we have seen that, in the absence of knowing the Risk Treatment Plan (RTP) from the mandatory risk analysis carried out, the systems that handle information classified in the grade of LD and systems in the HIGH category of the ENS can be considered equivalent.

Scenario 3 - System handling LD-grade CI and public cloud: this public cloud (multi-tenant) scenario, by analogy between systems handling LD-grade CI and ENS systems with HIGH category, is covered by the security measure **[op.nub.1] Protection of cloud services in** Annex II of RD 311/2022, of 3rd May, regulating the ENS, which must be complied with together with the other applicable measures.

Scenario No. 4 - System handling LD-grade CI and Public Cloud: this Public Cloud (multi-tenant) scenario is not envisaged in the first instance for systems handling SECRET, RESTRICTED or CONFIDENTIAL-grade CI, unless expressly authorised by the System Accreditation Authority.

Some public cloud providers offer single-tenant regions, for example, used in *SECRET* and *TOP SECRET* government clouds. They may also offer 'dedicated local zones' consisting of completely isolated zones located in Spain. In any case, these procurements for specific application to systems handling information classified above DL must be consulted in advance with the System Accreditation Authority.

4.4.2 National Security Framework (ENS)

4.4.2.1 Introduction to ENS

The Spanish legal system has Royal Decree 311/2022, of 3rd May, which regulates the National Security Framework (ENS), which affects the information systems of the entire public sector without exception, as well as the suppliers that provide solutions or provide services supported by electronic means.

The ENS aims to protect the information systems that support public services, together with the sensitive information they handle, by applying security measures based on the required security risk analysis and the category of these systems. This category may be BASIC, MEDIUM or HIGH.

As contemplated in the security measure **[mp.info.2] Qualification of the information,** to qualify the information, the legal provisions of the laws and international treaties of which Spain is a member and their applicable regulations shall apply in the case of classified material. The value to be used in the case of non-classified information would be OFFICIAL USE for information with some type of restriction in its handling due to its sensitivity and confidentiality.

In short, specific security measures must be established, depending on the level of security of the information in question, or its classification, in relation to the processing carried out with respect to it. As a result, it is necessary to adopt criteria or a rating scale (or classification, in the case of classified information based on the OSA or international treaties) that allow the security requirements to be adjusted to those criteria. An example might be to classify the information as 'OFFICIAL USE', while at the same time determining some scope of distribution or dissemination of the information, such as 'public', 'internal use', 'restricted', etc.

4.4.2.2 Criterios de externalización en la Nube

The Cloud Service Providers (CSP), when acting as a service provider to the public sector or its suppliers, must comply with the provisions of the ENS. This compliance is evidenced by having the mandatory ENS Compliance Certification, regardless of having other certifications based on international standards such as, for example, the ISO standards. There is currently a large number of ENS-certified CSPs, many of them in the HIGH category.

The Annex II of Royal Decree 311/2022, which regulates the ENS, contains the security measure **[op.nub.1] Protection of cloud services,** specifically for services provided in this modality, which details the basic requirements and mandatory reinforcements that must be adopted according to the category of system established by the ENS.

It should be noted that the fact that a CSP has obtained ENS Compliance Certification for HIGH category does not necessarily mean that any service it offers is ENS Compliant, just as a certification against an old version of the ENS may be outdated in some respects, for two (2) reasons:

- The first is the concept of the 'scope' of the provider's certification, which could be limited to a certain subset of the totality of services offered by the CSP: if the Cloud customer chooses other excluded services, these will not be covered by the CSP's ENS Certificate of Compliance.

- The second corresponds to the concept of 'service catalogue', which implies compliance with the ENS for a certain category if the Cloud customer contracts at least a number of services (such as the choice of two DPCs in different areas for the provision of the Cloud service, together with the option of replication between the two for availability purposes): if the customer does not contract a necessary service from the catalogue, it will not comply with the ENS as it does not meet all the requirements determined by the standard.

4.5 Personal data protection and related legislation

4.5.1 General Data Protection Regulation (GDPR)

Cloud Computing, depending on the geographic area or jurisdiction where the CSP's DPCs and consequently the customer organisation's data are located, may involve an International Data Transfer (IDT).

In relation to transfers of personal data to third countries or international organisations, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) states, in its Article 45 on transfers based on an adequacy decision, that a transfer of personal data to a third country or international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation concerned ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

At the time of writing, the European Commission has recognised fourteen (14) countries as providing adequate protection: Andorra, Argentina, Canada (only for organisations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom under the GDPR and LED, United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.

With the exception of the United Kingdom, these adequacy decisions do not cover exchanges of data covered by Article 36 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

There are other possibilities to legitimise TID, such as the third country or international organisation providing adequate safeguards, provided by means of instruments listed in Art. 46 of the GDPR on transfers by means of adequate safeguards (binding corporate rules, standard clauses, authorisation by the supervisory authority, codes of conduct, etc.).

4.5.2 Law 40/2015, of 1st October, on the Legal Regime of the Public Sector

Royal Decree-Law 14/2019, of 31st October, which adopts urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications, introduces a new art. 46 bis on the location of information and communications systems for the registration of data in Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, with direct implications for Cloud Computing.

The aforementioned article requires that, for reasons of public security, the information and communications systems for the collection, storage, processing and management of the electoral roll, the municipal registers of inhabitants and other population registers, fiscal data related to own or transferred taxes and data on users of the national health system, as well as the corresponding processing of personal data, be located and provided within the territory of the European Union. It also establishes that they may only be transferred to third countries when these comply with sufficient guarantees that they have been the subject of an adequacy decision by the European Commission, or when so required in order to comply with the international obligations assumed by the Kingdom of Spain.

4.5.3 Law 39/2015, of 1st October, on the Common Administrative Procedure for Public Administrations

Similarly, Royal Decree-Law 14/2019, of 31st October, which adopts urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications, introduces the new paragraph 3, which is added to both Article 9 and Article 10 of Law 39/2015, of 1st October, establishes the obligation that, in relation to the systems provided for in letter c) of paragraph 2 of Articles 9 and 10, the technical resources necessary for the collection, storage, processing and management of such systems must be located in the territory of the European Union, and in Spanish territory in the case of special categories of data referred to in Article 9 of Regulation (EU) 2016/677 of the European Parliament and of the Council, storage, processing and management of such systems must be located in the territory of the European Union, and in Spanish territory in the case of special categories of data referred to in Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

Subject to the exceptions introduced by law, these data may not be transferred to a third country or international organisation and, in any case, shall be available for access by the competent judicial and administrative authorities.

5. Data spaces

A data space is an ecosystem that allows diverse actors to share data in a voluntary and secure manner, following integrated governance, legal, organisational, regulatory and technological mechanisms, within an environment of sovereignty, trust and security for all participants.

Data spaces are thus conceived as (technologically) cyber-secure, **(digitally) sovereign** and (functionally) interoperable environments for sharing and exploiting data, while respecting common European standards and frameworks.

The concept of sovereignty is key, understood as the ability of a participant to maintain control over its own data by expressing the terms and conditions that will govern its permitted uses.

For more information on data spaces, which will often rely on the Cloud, see the guide **"CCN-STIC 813 Ciberseguridad de Espacios de Datos" (CCN-STIC 813 Cybersecurity of Data Spaces).**

6. Technical, organisational and contractual measures of each CSP

The following sections describe the measures considered by different public, private, or hybrid cloud providers. The following sections describe the measures considered by different public, private, or hybrid Cloud providers to meet the digital sovereignty requirements described above, as well as their vision in this regard, all with the purpose of facilitating the decision making process for the reader of this guide.

In view of the extensive documentation provided by the different suppliers, the following sections are the result of a significant exercise of synthesis and simplification. We therefore recommend contacting the CSPs themselves for more detailed information than that summarised here, in alphabetical order.

6.1 Amazon Web Services (AWS)

AWS has published its **Digital Sovereignty Commitment**, ensuring that the sovereignty controls and functionalities that AWS considers to be state-of-the-art are applied to all AWS CSCs for application to the cloud services offered.

Although, according to AWS, there is no single definition of digital sovereignty, it has drawn such a concept based on the following aspects:

Data sovereignty includes:

- **Data residency:** The CSC wants to know where all its data is and control where that data is stored and transferred, at all times.
- **Access restriction for operators:** The CSC wants to ensure that neither AWS nor any foreign government can access its data in the cloud.

Operational sovereignty includes:

- **Resilience and survivability:** The CSC wants to ensure that it can maintain operations despite potential geopolitical instability (e.g. foreign influence), natural disasters or technical failures.
- **Independence:** The CSC wants your organisation to prosper. It wants to contribute to the economic and social fabric of its country by developing technical capacities and infrastructure.

Of course, this is a generalisation, as digital sovereignty requirements vary across organisations and countries, with digital sovereignty policies in some countries still in their infancy, despite their rapid evolution.

6. Technical, organisational and contractual measures of each CSP

According to AWS, CSCs so far generally take three approaches to meet their digital sovereignty requirements beyond the standard public cloud:

- **On-premises:** some customers choose to delay innovation on global cloud platforms, stall projects or implement in-house. Risk: slower pace; reduced access to innovation; higher costs; sometimes less resilience; etc.
- **Hybrid:** some customers split workloads between public cloud and on-premises. Risk: higher complexity, higher costs, less access to capabilities, sometimes less security and less resilience.
- **Custom Cloud:** AWS offers several cloud regions created to address national and legislative requirements, such as GovCloud regions, "secret" or "top secret" regions in the US, or the recently announced creation of a new region in the European Union. It also offers **local dedicated zones,** which are a type of infrastructure that AWS manages in its entirety and is created for the exclusive use of CSCs. It is located in the data centre specified by the CSC to meet the regulatory requirements to which it is obliged. Such DPCs can be customer-owned (on-premise) or provider-owned (housing or colocation).

Hybrid and **'custom cloud'** options, according to AWS, represent a compromise between the CSP and the CSC and can lead to additional complexity and costs, as well as reduced speed, agility, access to innovation and resilience, by limiting the number of cloud-native services that are deployed.

AWS has the NITRO system, which powers all Amazon Elastic Compute Cloud (Amazon EC2) instances and provides a strong physical and logical security boundary to enforce access restrictions and **sovereignty by design and by default**, so that no one, including AWS employees, can access customer data running on Amazon EC2.

CSCs also have **control over the location of their data.** In Europe, customers who must comply with data residency requirements have the option of implementing them in any of the eight existing regions (Spain, Ireland, Frankfurt, London, Paris, Stockholm, Milan, and Zurich).

AWS and its customers exercise shared control of the IT environment. **Security is therefore a shared responsibility.** When it comes to managing security and compliance in the AWS cloud, each party has different responsibilities. The CSC's responsibility depends on the services it uses. However, in general customers are responsible for building their IT environment in a way that is in line with their specific security and compliance requirements.

AWS recommends that CSCs carefully consider and analyse the services they intend to select, as their responsibilities vary depending on the services they use, the integration of these services into their IT environment, and applicable laws and regulations.

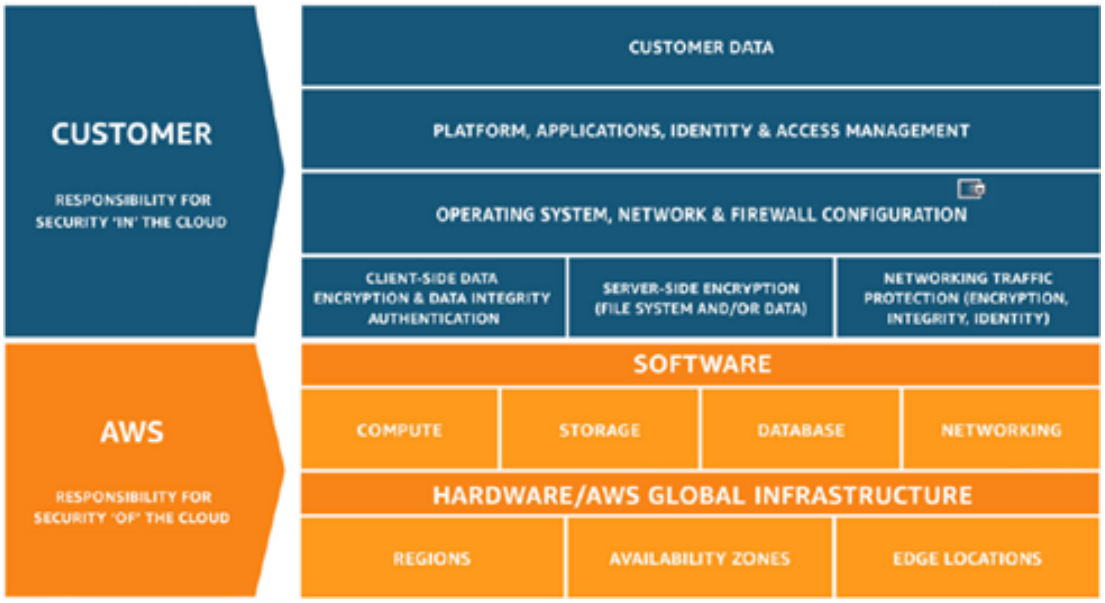


Figure 3.- Shared responsibility

CSCs can enhance security, or meet more stringent compliance requirements, such as **digital sovereignty requirements,** by using the **technical, organisational and contractual measures** detailed below.

6.1.1 Measures to meet digital sovereignty requirements

6.1.1.1 Technical measures

Firstly, the technical measures that apply to the services offered by the CSP must be considered in order to meet the requirements of digital sovereignty:

CSP employees do not access customer data: Verifiable control of access to data

On the one hand, we have the **classic Virtualisation** which:

- Allows the operator to access the host hardware.
- Networking, storage and monitoring run on the same hardware that runs the clients' virtual machines.
- Decreases performance and resources available to virtual machines.

On the other hand, we have **Amazon EC2 virtual machines** offered by AWS where:

- *The Trusted Computer Base* has been significantly reduced.
- All network virtualisation, storage and monitoring functions run on independent, isolated and secure hardware.
- All administrative access, including that of CSP employees, has been removed.
- There is only one small hypervisor on the host.
- NITRO provides protection of CSP operators and eliminates direct access to system memory.

AWS also offers **dedicated server and non-virtualised** EC2 instances where:

- There are all the advantages of NITRO, but without the hypervisor.
- CSCs can deploy applications that use physical hardware resources directly on the AWS infrastructure.

Encryption and control of encryption keys are under the control of the customer and with the ability to encrypt everything anywhere

All AWS services that store CSC data offer the possibility to encrypt it. Some of their features are:

- **Data-at-rest encryption functionalities,** available in most of the services offered.
- **Flexible key management options** allow you to choose whether you want the CSP to manage the encryption keys or allow the CSC to maintain full control over its own keys.
- **Dedicated hardware-based cryptographic key storage,** allowing it to meet security requirements. If the CSC has a regulatory need to store and use its encryption keys outside the cloud, it can use the external key store Key Management Service (AWS KMS).
- **Encrypted message queues to transmit sensitive information,** using Amazon Simple Queue Service (SQS) server-side encryption (SSE).

Infrastructure security

Several security features and services are available to enhance privacy and control access to the network. Some of them are:

- **Network firewalls built into Amazon Virtual Private Cloud (VPC),** allowing you to create private networks and monitor access to instances or applications. Customers can control encryption in transit between AWS services using TLS.
- **Automatic encryption of all traffic flowing over AWS global and regional networks between AWS-protected facilities.**
- **Connectivity options that allow private (or dedicated) connections to be made** from the local CSP environment.

6.1.1.2 Organisational measures

Secondly, organisational measures such as policies, procedures, guidelines or standards, which enable the organisation to create processes, mechanisms or controls that ensure the appropriate level of security for the risk, should be considered. The following sections describe the organisational measures that AWS offers through services and functionalities that will help to meet digital sovereignty requirements:

Control of the location of data (Data Sovereignty)

CSCs always have control over the location of their data in the following ways:

- **The CSC can determine where its data will be stored,** including the type and geographic region of storage.
- **The CSC can choose the security status of your data.** AWS offers customers encryption features to protect their content in transit and at rest, and gives you the option to manage your own encryption keys.
- **The CSC can manage access to its data and AWS services and resources through the** users, groups, permissions and credentials under its control.

AWS announced in October 2023 the launch of the **AWS European Sovereign Cloud,** a new cloud exclusively for the European Union, designed to help public sector organisations and customers in highly regulated sectors meet their evolving digital sovereignty needs. Only CSP staff, resident and located in the EU, will have control of day-to-day operations, including access to data centres, technical support and customer service.

For CSCs with **enhanced data residency needs,** the AWS European Sovereign Cloud will allow customers to retain within the European Union all the metadata they create (such as roles, permissions, resource tags), accounts and configurations they use to run AWS.

Security in Multi-tenancy environments

CSPs offer multi-tenancy services that place multiple customers' applications and data on the same physical infrastructure.

CSP customers can leverage some or all of the capabilities detailed below to meet, and sometimes exceed, the security provided by physical separation at the facility:

- **Unified authentication and authorisation:** A robust, granular authorisation and authentication model common across all AWS services that integrates with local user identity management systems.
- **Rich monitoring and logging:** Deep, granular logging services for visibility into all API calls and resource state across AWS services. Current configuration and application events are centrally logged to quickly understand both the current security posture and a record of previous configuration states.
- **Virtual Private Cloud (VPC) and accompanying features:** VPC is a software-defined network that allows customers to create segmented or micro-segmented network domains to isolate the flow of traffic between different AWS computing environments and services, and to join segments where necessary in a secure and constrained manner.
- **Encryption of data at rest and in transit:** Encryption options for all AWS storage services, powerful certificate creation and lifecycle management for encrypting data in transit. Secure key management (generation and storage).
- **Host and instance isolation:** Options to provision dedicated hypervisor-enabled or bare-metal architectures to keep CSC data on a physical computing host are not shared with other clients.
- **Serverless and containerised architecture:** Isolated execution environments provide a smaller, ephemeral execution environment to simplify security controls.

6.1.1.3 Contractual measures

Finally, thirdly, it details the contractual measures offered to comply with digital sovereignty requirements such as the General Data Protection Regulation (GDPR) or the National Security Framework (ENS):

Terms and Conditions / Privacy

According to AWS, a Service User Agreement, Processor Agreement, Service Level Agreements (SLAs), Acceptable Use Policy and Intellectual Property License are in place.

The AWS Terms of Service state that AWS personnel do not have access to customer data. The Service User Agreement includes a contractual commitment not to move customer data outside the region they have selected. And the privacy features of AWS services provide transparency about services that involve the transfer of customer data. We do not use customer data, or obtain information from customers, for marketing or advertising purposes.

International transfers

For transparency, the CSP has a list of services that involve a transfer of customer data on the AWS privacy features webpage.

Subcontracting

The CSP provides updated information on the subcontractors it has engaged, in accordance with the AWS GDPR Data Processing Annex (AWS ATD), to carry out customer data processing activities on its behalf (available on the AWS Subcontractors page).

There are three types of subcontractors:

- Entities **providing the infrastructure** on which the CSP services run.
- Entities **supporting specific AWS services** that may require these entities to process CSC data.
- Third parties that the CSP has contracted and that **perform processing activities** for specific AWS services.

Exit Plan

The CSP has numerous Open-Source based services and technology that enable it to define an AWS porting and exit strategy.

Clarifying Lawful Overseas Use of Data Act (CLOUD ACT)

The CLOUD Act *(USA Cloud Act-Clarifying Lawful Oversees Use of Data* amending the *Stored Communications Act)* allows US law enforcement agencies to access, on very specific and targeted occasions and for very specific purposes, to data hosted in CSCs. However, some relevant aspects of the application of the CLOUD Act should be qualified:

- The CLOUD Act does not apply only to CSPs, but applies to all providers of electronic communications or remote computing services operating in the US, regardless of whether those providers are based in the United States or in another country.
- The CLOUD Act does not grant US law enforcement unlimited or unrestricted access to data. Law enforcement may only request content from CSPs in two circumstances: (1) with the **consent of the customer** or (2) **with a warrant issued by a US court pursuant to US** criminal procedures. For a warrant to be issued, the court must be satisfied that there is probable cause to believe that a crime has been committed and that the evidence sought under the warrant is directly related to that crime.
- When a content request is received from law enforcement, it is carefully reviewed by the CSP for accuracy and compliance with applicable law. In cases where the CSP must act to protect customers, it will continue to do so. AWS has a history of challenging government requests for customer information as exaggerated or inappropriate for any reason. If required to disclose the contents of CSCs, AWS will continue to provide prior notice to such customers before disclosing the requested information to give them an opportunity to request protection from disclosure, unless prohibited by law.

The CLOUD Act is encryption neutral and cannot force service providers to decrypt customer communications or data. Additionally, it is important to note that AWS does not have access to encryption keys controlled and stored in HSM that are FIPS 140-2 level 3 compliant. It is also important to note that US courts have determined that **data belonging to US allied governments cannot be requested through the CLOUD Act, but through bilateral mechanisms established at international level.**

6.2 Google Cloud

As explained above, the definition of Digital Sovereignty is not unique and is not just about implementing a set of technological measures.

Google, in addition to launching its Digital Sovereignty technology proposal, which is outlined in this section, has carried out other actions in initiatives that are part of a strategic plan to improve and increase Digital Sovereignty in Spain, as they add value to the country's ability to control its own digital destiny.

The Open Cloud concept[6] of Google Cloud has a special relevance when talking about Digital Sovereignty. Google's commitment to open source adds unique Digital Sovereignty capabilities such as:

- Transparency in the source code of many of the services they run.
- Flexibility to deploy (and migrate if necessary) mission-critical workloads on or off public cloud platforms.
- Flexibility to develop and run apps from anywhere.
- Autonomy and control over infrastructure and data.
- Increases data survivability and reduces vendor lock-in.

6. https://cloud.google.com/open-cloud

'Cloud' security is the priority according to Google. However, this document does not detail the security measures and solutions that are available to customers who choose to bring their workloads to Google. Security services such as firewalls, Confidential Computing, key managers, HSM, encryption at rest, in transit and in use, API proxification, ability to choose the region where workloads are located, strong organisational policies on access control, roles, users, anti-DDoS measures, DLP, monitoring, controls over private networks, ... are all measures that form part of the Google Cloud Platform's basic security catalogue[7].

This document only includes solutions that have been specifically developed to provide its cloud services customers' data with digital sovereignty capabilities.

6.2.1 Google Cloud's approach to the Cloud Act

Like other technology and communications companies, Google receives requests from governments and courts around the world for customer information. Google Cloud has developed a transparent, fair and thorough process that complies with international best practices for data access requests from government agencies, including data access requests under the Cloud Act. Google provides a case-by-case response, taking into account different circumstances, legal requirements, customer agreements and privacy policies.

Google was the first cloud provider to publish periodic transparency reports[8] on government requests for customer information including requests for access to data under the US Cloud Act. Google has robust operational policies and procedures and other organisational measures in place that protect against unlawful or excessive requests for data by public authorities:

Redirection: If Google receives a request from a Government Agency to obtain customer data from the cloud based on the Cloud Act Google informs the government that it must issue the request directly to the organisation (i.e. the customer). This approach is aligned with the US government's policy (US Department of Justice) and the contractual obligations and commitments between Google and the customer.

7. https://cloud.google.com/solutions/security
8. https://transparencyreport.google.com/user-data/enterprise

Legal validity assessment: If, however, the government compels Google to respond to a request for customer data, a dedicated team of Google lawyers and specially trained staff will carefully review the request to verify that it is lawful, proportionate, and satisfies Google's requirements and policies. Google maintains a dedicated, dedicated, cross-functional team to evaluate and process requests for user data in a manner that respects the law and protects users' privacy and security.

All requests for user data must be processed and approved by team members before any data is made available. All requests are handled in accordance with the law and Google's policies and procedures. In addition, Google objects to, limits or modifies the request if it deems it to be overly broad, disproportionate or inconsistent with applicable law; Google objects directly if it deems it to be unlawful[9].

Customer notice and transparency: Google will notify the customer before its data is disclosed, unless such notification is prohibited by law, would obstruct a public authority from conducting an investigation, or would cause death or serious physical harm to a person.

Where prior notification by Google is prohibited under applicable law, it is Google's policy to notify the customer when any prohibition is eventually lifted, such as when a law or court orders disclosure or the prohibition period has expired. This notification is usually sent to the Google Cloud customer.

Customer Legal Action: Google will, to the extent permitted by law and by the terms of the governmental request, comply with a customer's reasonable requests with respect to its efforts to oppose a request, such as the customer filing an objection to disclosure with the appropriate authority, court and providing a copy of the objection to Google.

If Google notifies the customer of a governmental request for customer data and the customer subsequently files an objection to the disclosure with an appropriate court and provides a copy of the objection to Google, Google will not provide the data in response to the request.

9. https://services.google.com/fh/files/misc/government_requests_for_cloud_customer_data_google.pdf

6.2.2 Technological proposal for digital sovereignty

Having seen that the Digital Sovereignty proposal does not consist solely of a technological proposal, this section explains the proposed technological proposal This is not just about choosing controls that have already existed for years and exposing them as a Sovereignty solution. The approach has been to develop a new technological solution, with new products and services, innovating on how it is possible to obtain higher levels of security and independence in the Cloud than those obtained in on-premise deployments in many cases.

The proposal should be modular and scalable, allowing users to choose from a catalogue the level of Digital Sovereignty they need for each of their services, without having to invest more, but allowing the maximum levels of Digital Sovereignty in the services that require it without renouncing innovation and scalability.

Google understands that the solution offered in the Cloud must be based on a catalogue of products and services with the objective of allowing users to host, from public information to classified information of the highest level, passing through the intermediate levels, adapting the cost and complexity to each of the cases.

The different levels of information and recommendation on how to approach a solution with Google Cloud products and services is as follows:

	Pública	Sector Público ENS	Sin Clasificar Uso Oficial	Difusión Limitada	Confidencial+
GCP	✓	—	—	—	—
GCP-ENS	✓	✓	—	—	—
Controles Regionales	✓	✓	✓	—	—
Controles Soberanía	✓	✓	✓	✓	—
GDCH	✓	✓	✓	✓	✓

Figure 4.- Differentiated solutions according to levels of information sensitivity

In Google's proposal for Digital Sovereignty in Spain there are two (2) differentiated lines detailed below, a first connected proposal and a second, for heavily regulated workloads, completely disconnected. The following points provide an abbreviated description of the proposals:

6.2.3 Connected digital sovereignty

Google Cloud's connected proposition consists of a series of new products and services developed specifically to empower users with Digital Sovereignty capabilities without sacrificing the innovation, technological capabilities and economies of scale of the public Cloud.

6.2.3.1 Having a trusted partner

In the technology proposition, the trusted partner plays an important role as it is responsible for several key points of the proposition:

External key manager: It keeps in its data centres under its full control the key manager with which the data is encrypted in the Cloud. The CSP has no access to or control over these keys at any time.

Operations control: Controls, authorises and monitors all operations of CSP staff on the infrastructure supporting customer data.

Local support: Provides support from Spain and in Spanish for the CSP's customers in Spain. This means that the cloud service provider is not even aware in many cases of possible incidents that its customers may have, as they are solved completely autonomously by the trusted partner.

6.2.3.2 Technological solution

As mentioned above, the Digital Sovereignty technological solution must be a modular and scalable solution that allows the complexity to be adapted to the sovereignty requirements of each client.

In order to specify the technological solution proposed by Google, each of the products and services exclusively designed to provide Digital Sovereignty are listed below, from the lowest to the highest level of requirements.

Google Cloud Platform (GCP)

Cloud service customers whose requirements are solely to host public or corporate information without any Digital Sovereignty requirements can use GCP's public cloud in its default configuration with high level of security, service and innovation.

The security measures implemented by default in GCP include default encryption of all customer data at all times, high availability, permanent monitoring systems, best-in-class anti-DDoS protection, anti-ransomware systems, Chronicle SIEM/SOAR, VirusTotal, Mandiant, etc.

Google Cloud Platform (GCP-ENS)

When the cloud services customer needs to comply with the requirements of the National Security Framework, the solution could not be simpler as it is implemented on top of GCP, using all the above protection mechanisms and enhancing security and compliance with the necessary configuration to comply with the ENS provisions including those of HIGH category.

Importantly, the scope of Google Cloud ENS Conformance Certification includes all GCP data processing centres worldwide, as well as many services, including Sovereignty services. Digital Sovereignty and Artificial Intelligence services.

6.2.3.3 Regional controls

This service increases the level of data sovereignty, security and confidentiality and implements different controls over the public cloud. In addition to ensuring high category compliance with the ENS, it adds:

- EU residency checks so that data always remains within EU boundaries.
- Transparency of access, allowing customers full visibility into the operations of Google personnel over the infrastructure that supports their systems.
- TLS restrictions to ensure maximum security for data in transit.
- Restrictions on the use of services without guarantees of residence.
- Customer managed keys in the Cloud to encrypt data (CMEK).
- Transparency of access to keys (monitoring of the use of cryptographic keys)
- 'Confidential Compute' - Encryption in use.
- VPC controls, perimeter layer of protection of sensitive data.
- Google support with staff in the European Union.

6.2.3.4 Sovereignty controls

On top of the Regional Controls, the Sovereignty Controls are built, including all controls established on the public Cloud and maintaining the ENS compliance level of HIGH category.

- **External Key Management:** Allows the encryption keys of the information to be managed externally to the cloud, so that Google cannot access the information at any time because it is cryptographically protected.
- **Justification of access to keys:** Offers the possibility of defining (externally to Google) the reasons for which it is possible to access a key, enabling and disabling keys autonomously to Google Cloud.
- **BYOID:** Allows the use of existing, external identities with sovereignty services.

For the highest level of connected sovereignty, the trusted partner is involved as detailed in previous sections. The trusted partner offers the following controls and guarantees:

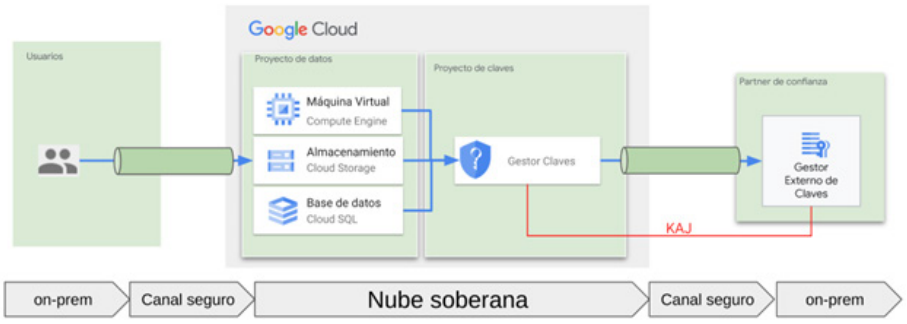
- **External key management:** Through a managed service, the trusted partner offers the management of external keys with all the guarantees, including the justification of access to the keys and the monitoring of the use of these keys.
- **Support from Spain and in Spanish:** The trusted partner offers specialised support so that Google staff do not access the services, even in the case of customer problems in Spain.
- **Access Control:** When Google Cloud personnel (personnel always located in the European Union) need to perform any operation that may involve access to client systems, they will need prior approval, cryptographically signed with an external key, before being able to access the operation.
- **External Key Management:** External Key Management through Cloud EKM[10] (External Key Manager) is a fundamental piece of our connected Digital Sovereignty technological proposal. Cloud EKM is included in the CPSTIC Catalogue (CCN-STIC-105) in May 2023.

10. https://cloud.google.com/kms/docs/ekm

Cloud EKM allows keys to be created and managed completely external to GCP, in the trusted partner's data processing centre, and to use those keys to encrypt information in the cloud. In this way, information on the GCP platform is encrypted with a key that is not in the cloud, allowing the customer or partner to control who, when and for what purpose that key is accessed and therefore the information it protects.

EKM allows you to create keys for symmetric encryption and asymmetric keys for digital signature, all outside the cloud at all times. Another of EKM's functionalities is KAJ (Key Access Justification). KAJ allows you to define in the external key manager, the reasons why access to the keys is allowed at a given time, allowing the customer or partner to define when Google can access each of the keys and for what purpose.

The diagram below shows at a very high level, how external encryption could be used in three (3) different services, as an example.



6.2.4 Digital sovereignty disconnected

For customers with regulated needs such as the use of classified information (Confidential grade or higher) Google Cloud has created, within the Google Distributed Cloud, its disconnected version:

6.2.4.1 Google Distributed Cloud Hosted (GDCH)

According to Google, unlike other third-party solutions that may appear similar, GDCH is a completely disconnected cloud, designed to run sensitive workloads, supporting customers with strict data residency, security and privacy requirements. GDCH requires no connection to the CSP or any other network for operation.

GDCH includes the hardware, software, local control plane and operational tools needed to deploy, operate, scale and secure a complete managed cloud. Customers in regulated industries such as government, financial services, healthcare and manufacturing have the ability to meet business priorities and help modernise even their most sensitive or confidential workloads.

Main functions of GCDH

The main functions of GDCH include:

- **Total isolation:** GDCH requires no connectivity to the Google Cloud or the public Internet to manage infrastructure, services, APIs or tools, and is designed to remain in perpetuity.
- **Integrated cloud services:** GDC Hosted offers advanced cloud services, including many of our data and machine learning technologies, AI solutions, OCR, Speech-to-Text and enables a catalogue of independent software vendor (ISV) applications across our marketplace.
- **Open ecosystem:** Designed around Google Cloud's open cloud strategy. It is based on the Kubernetes API and uses industry-leading open-source components in the platform and managed services.
- **Flexible hardware options:** Provides customers with industry-leading flexibility for hardware, including pervasive processing and GPUs. Customers can start with as few as four racks and grow as their workloads grow.
- **Configurable operations:** The operating model can be configured to suit the unique needs of each client.

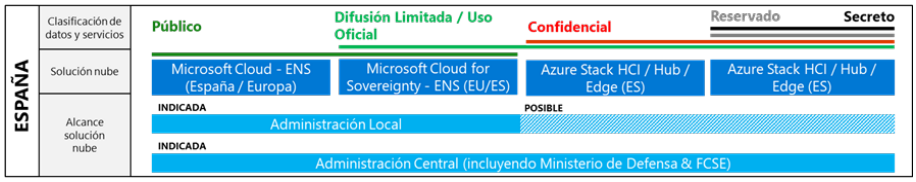
6.3 Microsoft Cloud

6.3.1 Indroduction

Microsoft has been in Spain for more than 35 years and has made various investments in training, digitisation and improvement of the ecosystem of technology companies. It was the first Cloud provider to obtain the certificate of conformity for the National Security Framework (2016) and has recently obtained the renewal **(RD 311/2022)** HIGH category being the first and only ones to include a Cybersecurity service supported by Artificial Intelligence.

6.3.2 Technical measures for Digital Sovereignty

Microsoft's approach to digital sovereignty follows a line based on levels of information classification. The approach is to provide the highest possible security and innovation for each classification level with Cloud solutions.



This approach according to the level of classification of the information allows in each case to adapt to the needs of the CSCs by adding the safeguards developed by the engineering teams and aligned with the requirements of the different regulations to provide greater security and transparency.

6.3.2.1 Microsoft Cloud

Microsoft Azure, Microsoft 365, Microsoft 365 for Education, Microsoft Dynamics 365 and Microsoft Power Platform have been audited and found **compliant with the requirements of Royal Decree 311/2022 of 3rd May, which regulates the National Security Framework, complying with the provisions defined in the HIGH category.**

Microsoft has more than 170 Cloud services under the scope of this Certificate of Conformity, including Computing, Storage, Networking, Key Management, Productivity, Security, Artificial Intelligence and the services used by the Microsoft Cloud for Sovereignty solution. All regions located in the EU + EFTA (including the region of Madrid - Spain) are also within the scope of this certificate of conformity.

6.3.2.2 Microsoft Cloud for Sovereignty (ENS)

Microsoft Cloud for Sovereignty is a new Cloud solution generally available to all customers from December 2023. This solution is made up of different pieces developed and available exclusively for customers who require digital sovereignty solutions. Microsoft Cloud for Sovereignty provides different assets:

- Sovereign Landing Zone (SLZ) deployment and configuration tool to restrict and configure services and regions and apply sets of policies mapped to existing regulations.
- Sovereign Landing Zone (SLZ) lifecycle management tool that enables pre-deployment assessments, identification of redundancies, conflicts and out-of-policy items, and configuration integrity monitoring.
- Sets of policies mapped to existing regulations and industry standards, including ENS level HIGH (available from 17/05/2024)[11].
- Compliance monitoring tools for such policies through Defender for Cloud providing a compliance scoring system.
- Dedicated key management (single tenant) via Azure Key Vault Managed HSM (FIPS 140-2 Level 3) with full control of the security domain by the partner / CSC, removing the CSP (Microsoft) from the chain of custody while ensuring Microsoft Cloud SLAs and avoiding the security issues of interfacing with external systems.
- Confidential computing through Azure Confidential Computing for the protection of data and code, as well as entire virtual machines while in use.

11. https://learn.microsoft.com/es-es/azure/governance/policy/samples/built-in-initiatives#regulatory-compliance

- Transparency logs[12] to give visibility of operations performed by Microsoft engineers. Both operations required by the partner / CSC and operations performed by the CSP (Microsoft) are covered. All accesses are logged with information on subscription, day/time of access, service accessed, engineer role, location (workplace) of the engineer and access time. This information is also accessible for 90 days.

Third in confidence

For the Microsoft Cloud for Sovereignty solution, Microsoft proposes the figure of the trusted third party, the partner. This is responsible for operating the CSC services provided by the CSP (Microsoft Cloud).

- Operates the customer's Cloud infrastructure.
- Gives technical support to the client.
- Manages the encryption keys through the Azure Key Vault Managed HSM service, having full control of the security domain where the encryption keys will be stored, thus removing the CSP (Microsoft) from the chain of custody.
- Manages the customer's Sovereign Landing Zone (SLZ), its policies and access to transparency logs.

6.3.2.3 Azure Stack HCI / Hub / Edge

For the highest classification levels, Microsoft has three types of services for hybrid/private cloud environments.

- **Microsoft Azure Stack HCI (Hyperconverged)** and is a leader in Gartner's distributed hybrid infrastructure quadrant[13]. It allows any application, virtual machine or container-based workload to run anywhere with a consistent experience with the Azure control plane in a semi-disconnected mode (a connection is required every 30 days). Containerised AI services are available including Generative AI services.

12 https://learn.microsoft.com/en-us/industry/sovereignty/transparency-logs#details-covered-in-transparency-logs
13. https://azure.microsoft.com/es-es/blog/microsoft-recognized-as-a-leader-in-2023-gartner-magic-quadrant-for-distributed-hybrid-infrastructure/

- **Microsoft Azure Stack Hub** extends Azure to run applications in the local environment (CSC's own data centres) by being able to deploy Azure services in its data centre in fully disconnected mode. Azure Stack Hub is approved for use by the CCN-CERT[14] Certification Body. It provides containerised Artificial Intelligence services including Generative AI services.

- **Microsoft Azure Stack Edge** extends the capabilities of Azure Stack, allowing workloads to be run and data to be retrieved at the edge, where data is created, using dedicated hardware-as-a-service. It includes ruggedised formats and is also certified by the CCN-CERT[15] Certification Body . It provides containerised Artificial Intelligence services including Generative AI services.

6.3.3 Organisational measures

Microsoft has an organisational framework based on security policies, operating procedures, internal processes and compliance with market standards to ensure customer security. These measures are detailed below:

6.3.3.1 Data monitoring

- Microsoft only uses customer data to provide you with the agreed services and for purposes related to the provision of those services.

- It does not share CSC data with advertisers or for marketing purposes. This policy is supported by service agreements and the adoption of the international code of practice for privacy in the cloud, ISO-IEC 27018.

- Microsoft adheres to strict privacy and security standards and removes CSC data from systems under its control, overwrites storage resources before reuse and purges or destroys retired hardware.

14. https://aka.ms/AzureStackOc
15. https://aka.ms/AzureStackOc

6.3.3.2 Residence and data security

- The CSC always decides in which Microsoft Cloud region to place its data (it has more than 65 regions worldwide, including the Madrid - Spain region).
- The CSC decides which encryption mechanisms it uses in Microsoft Cloud services.
- The CSC defines the roles and permissions (RBAC) for its services in Microsoft Cloud.
- For services under the EU Data Boundary initiative[16], Microsoft stores and processes CSC and personal data within the EU.
- Microsoft protects its customers' data at rest (its data centres), in transit (between the CSC and Microsoft, and between Microsoft's data centres) and in use (if contracted by the CSC) with advanced encryption.

6.3.5 Contractual measures

6.3.5.1 General Data Protection Regulation (GDPR)

Microsoft is committed to comply with the GDPR. Microsoft's contractual commitments with respect to the GDPR (GDPR Terms) are set out in the annex to the **Data Protection Addendum entitled "Terms of Compliance with the General Data Protection Regulation of the European Union"**[17]. By these terms Microsoft commits to the requirements for processors in Article 28 of the GDPR and other related articles.

6.3.5.2 Clarifying Lawful Oversees Use of Data (CLOUD Act)

Microsoft, like any company operating in the US, including European companies, is subject to compliance with the Clarifying Lawful Oversees Use of Data Act (CLOUD Act). Through the CLOUD Act, content can be requested from service providers only when the subject has given consent or with a court order, or pursuant to a previously agreed bilateral agreement.

---

16. https://learn.microsoft.com/es-es/privacy/eudb/eu-data-boundary-learn
17. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=31

The CLOUD Act does not provide unrestricted access to personal data. Microsoft makes a number of contractual commitments with respect to this Act:

- Microsoft defends its customers' data through clearly defined and established policies and processes, contractual commitments and, if necessary, the courts. First, by **redirecting any government requests for data to the customer.**
- If Microsoft receives a request for data that belongs to a customer, it **will notify you promptly and provide you with a copy of the request unless it is legally prohibited from doing so.**
- In addition, Microsoft **will use its best legal efforts to challenge the disclosure request on the basis of** any legal deficiency relating to the requestor's law or on the basis of any conflict with European Union law or the law of the applicable Member State.
- In the event that, after having followed the steps described in the preceding paragraphs, Microsoft or any of its affiliates is still required to disclose personal data and subject to the conditions set out in the Data Protection Addendum[18], **Microsoft will indemnify a data subject in respect of material and non-material damage** caused to him or her as a result of a disclosure, by Microsoft of personal data of the data subject that has been transferred in response to a request from a public authority or governmental body outside the European Union or the European Economic Area in breach of Microsoft's obligations under Chapter V of the GDPR.
- Microsoft does not grant and has never granted access to personal data of EU public sector and business sector customers. Nor does it provide any government with Microsoft's encryption keys or the ability to break its encryption mechanisms.

6.4 Oracle

6.4.1 EU Sovereign Cloud

Oracle's approach to digital sovereignty is driven by the **EU Sovereign Cloud** solution, which offers customers access to more than 100 services that are the same as Oracle's commercial public cloud.

18. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=31

The same applications and workloads can be run on Oracle EU Sovereign Cloud, with no new skills or operational processes required.

Currently, there are two (2) EU Sovereign Cloud regions, one in Spain and one in Germany. **Both are independent of Oracle's commercial and government cloud regions.** This independent EU cloud architecture simplifies and strengthens digital sovereignty and controls.

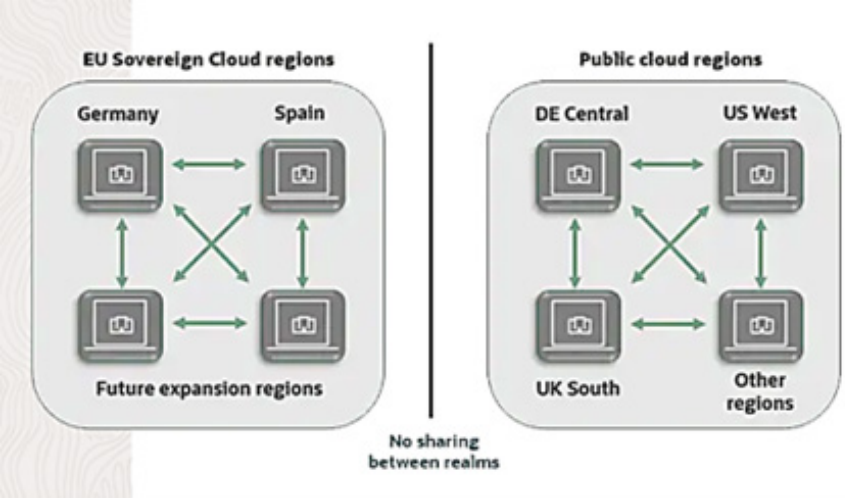


Figure 6.- Distinction between EU Sovereign Cloud regions and Public Cloud regions

6.4.2 Advantages of the Sovereign Cloud

Customer deployments are faster and take less risk with data residency and containment in the EU by default, without relying on complex policy-based tools to configure them.

Customers can use the two Cloud regions in Madrid and Frankfurt, both separated by about 1,500 km, for redundancy and disaster recovery. Each Oracle Cloud region has at least three fault domains, which are clusters of hardware that form virtual data centres to provide local high availability and resilience to hardware and network failures.

The **EU Sovereign Cloud domain** differs from other Cloud offerings by being a domain designed for EU data, located in the EU, operated entirely by EU residents and with physical and logical access restricted to EU residents.

Oracle personnel providing customer support, data centre support and data centre operations are located throughout the EU. The hardware and assets used for the EU Sovereign Cloud are owned, operated and managed by a separate legal entity.

6.5 Other public, private or hybrid Cloud providers

Future updates of this guide are open to other Cloud Service Providers (CSPs) to contribute their knowledge and views on digital sovereignty in terms of data protection mechanisms in the Cloud in order to maintain control over their data.

Annex 1. Contractual clauses and cloud computing

1.1 Introduction

Cloud computing represents a departure from the traditional IT service delivery model. An important part of the successful migration to the Cloud is the formalisation of the contract(s) (service delivery, access to personal data, etc.) between the provider (CSP) and the customer organisation (CSC).

1.1.1 Contractual regulation of service provision

Any provision of services, and cloud computing is no exception, requires a contract to regulate the relationship between the CSP and the CSC (in this case, the contractor). We will distinguish:

- **The terms of** the contract, which should clearly define the position of each party, as well as their responsibilities and obligations, usually including issues relating to the security of customer information held by the supplier.

- **Terms of use,** which are responsible for defining the most important technical specifications related to the delivery and quality of service. They are usually set out in documents called Service Level Agreements (SLAs) and, among other issues, establish the levels of performance and availability guaranteed by the provider.

While commercial contracts are always negotiated, in the case of CSPs there is often no such alignment of positions. CSPs usually clearly display on a web portal the conditions under which they provide their service and it is up to the customer to adhere to them (adhesion contracts). Consequently, a good advice is to negotiate the contract whenever possible or, failing that, to carefully study each of the clauses proposed by the different providers, until the agreement that best meets the customer's needs is found.

CSP customers may differ in typology (public sector or private sector organisations), size (private sector from μSMEs to large companies; public sector from small to large organisations) and service usage (high turnover customers and relatively irrelevant customers in terms of turnover), which will determine their bargaining power. This aspect is very relevant from a legal point of view, as the future relationship between a CSP and its customers will be regulated by means of such a contract. Due to the lack of specific regulations, the reciprocal functions and obligations will be set out in general contract clauses, drawn up unilaterally by the CSP and accepted by customers without modification (commonly), or negotiated in specific agreements.

It should be noted that even when a customer cannot negotiate different terms of a contract with a specific CSP, the customer is still free to choose between the different offers on the market. Therefore, in the case of a small organisation, the following recommendations regarding specific contractual clauses should be understood as facilitators of choice between different market offers.

1.1.2 Detailed analysis of each clause

1.1.2.1 Conformity with the ENS

If the cloud-hosted services fall within the competences of the procuring public entity, it is imperative that the information systems on which such services are based comply with the provisions of the ENS, the security levels in each dimension and the security category previously determined by the procuring entity.

The above implies the need to verify that the CSP systems concerned have the corresponding ENS Declaration of Conformity (only applicable to Basic category information systems) or ENS Certification of Conformity (mandatory for Medium and High category systems). In the latter case, if the systems do not have the Certification, they must be assessed by an ENS Certification Body accredited by ENAC to confirm compliance, in accordance with the provisions of the Resolution of 13th October 2016, of the Secretary of State for Public Administrations, approving the Technical Instruction on Security in accordance with the National Security Framework, after having satisfactorily passed a Security Audit, regulated in the Resolution of 27th March 2018, of the Secretary of State for Public Administration, approving the Technical Instruction on Security Auditing of the Security of Information Systems.

1.1.2.2 Information security and protection of personal data

Special attention should be paid to this clause, the purpose of which is to ensure that the CSP can provide sufficient security measures, both technical and organisational, for the processing of personal data carried out on the basis of the provision of its services, while ensuring compliance with the client's legislation on the matter (such as the RGPD and the LOPDGDD).

For greater assurance, it would be good to state in the service provision contract that the CSP has information security certifications (e.g. ENS) perhaps complemented by ISO/IEC 27018:2019 Code of Practice for the protection of Personally Identifiable Information (PII) in the cloud or any other international standard. Particular attention should be paid to the scope of certification, which should cover the whole set of services being procured, as all standards allow for partial certifications. It should be remembered that the certifications obtained by a CSP are not eternal, being subject to a renewal process from time to time based on an audit carried out by an accredited certification body (CB) (in Spain by ENAC) and, with regard to ISO standards, annual follow-up audits. This means that it should be verified annually that the CSP maintains the necessary certifications.

Usually, in addition to a data protection clause in the service provision contract with the CSP, an additional specific processor contract is concluded in order to comply with Art. 28 of the GDPR which states that "1. *Where processing is to be carried out on behalf of a controller, the controller shall choose only a processor providing sufficient guarantees to implement appropriate technical and organisational measures, so that the processing is in compliance with the requirements of this Regulation and ensures the protection of the rights of the data subject*".

1.1.2.3 Territoriality of data and possible International transfers

This clause shall reflect the territoriality of the Data Centres (DPC) where the information of the customer contracting Cloud services will be located.

If such a transfer is to a third country, e.g. outside the EEA (European Economic Area), it may have important legal consequences, as it will be considered an international transfer of data. In such a case it would only be considered feasible if an Adequacy Decision is available on the basis of Art. 45 of the GDPR on international data transfers, which states *"1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or a specific sector or sectors within that third country, or the international organisation concerned ensures an adequate level of protection. Such a transfer shall not require any specific authorisation"*.

According to the European Commission, at the time of writing, there are 14 countries that have been recognised as adequate for the transfer of personal data from the EU: Andorra, Argentina, Canada (only for organisations subject to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, United Kingdom and USA (for the EU-US data privacy framework, which entered into force on 10 July 2023). It should be noted that these adequacy decisions can be reviewed or revoked by the European Commission at any time if it considers that the level of protection is no longer sufficient.

1.1.2.4 Applicable legislation

Applicable law is the body of laws and regulations with which the contract between the CSP and the CSC must comply.

Each country has specific restrictions and requirements under legislation applicable to the data, mainly if they are of a personal nature.

The contract should reflect the law to which the data and its processing will be subject in relation to the client, who acts as the Data Controller. The CSP acts as the Data Processor.

1.1.2.5 Jurisdiction to which the parties submit

Another relevant aspect is the applicable jurisdiction in relation to discrepancies between the parties (CSP and client) during the life cycle of the contract that regulates the provision of Cloud services. Given the universality of many CSPs, this clause should reflect the jurisdiction to which the parties submit, as well as outlining the maximum identifying details of each organisation so that the customer is not helpless when they need to assert their rights.

It should be borne in mind that this may result in null and void liability clauses, depending on the applicable law governing the contract. If the law is Anglo-Saxon, it accepts limitations of liability of CSPs and, where appropriate, determines financial compensation based on the amount paid by the customer when contracting the service. If the law is continental, it allows limitation of liability for negligence, but not for fault or wilful misconduct.

It is not always easy to obtain jurisdiction in one's own country. In practice, the final decision depends on the bargaining power of the parties, so that the CSP or CSC that enjoys a preponderant position ends up imposing the conditions that are most convenient for it.

1.1.2.6 Confidentiality

The CSP's obligations regarding confidentiality must be contemplated, i.e. that it will not disclose our data to third parties. The clause will state that all CSP employees or collaborators (technical, administrative, support or maintenance staff) who, due to operational matters of the DPC, have or may have access to the client's data, will have signed a confidentiality clause. The CSP will therefore be liable for any wilful or negligent action on their part. This aspect is guaranteed if the CSP has the ENS Conformity Certification, but it is not superfluous for it to be reflected in the contract.

Another key point to take into account in the confidentiality clause is the limitation of the circumstances in which the service provider may disclose the information to third parties. Although the jurisdiction that will govern the contract may contain specific provisions in this regard, it is advisable to limit the disclosure of data for the purposes of complying with legal obligations or the requirements of competent authorities.

In any case, it should be noted that the disclosure of data or information must be the minimum necessary to comply with any legal obligations or requirements. Whenever possible, the CSP shall undertake to notify the customer as soon as possible of such disclosure of data, indicating what data it has disclosed and to whom it has disclosed it. Another issue is that the service customer's data is encrypted at all times.

1.1.2.7 Intellectual and industrial property

The intellectual and industrial property clause is important to bear in mind. In its broadest legally enforceable sense, it refers to so-called copyrights, patents, trademarks and industrial design.

To generalise, it can refer to the fact that all the work that has been carried out during the life cycle of the cloud services contract, based on the utilities provided by the CSP, are the intellectual property of the client or of third parties who have granted the right to use them by means of the corresponding licences. It must be stipulated that the data, App (applications), DDBB (databases) and other software tools that the client has placed in the CSP infrastructure are its property.

Depending on the Cloud service delivery model that has been contracted, this may be more or less difficult to determine:

- **Infrastructure as a Service (IaaS).** This delivery model is equivalent to contracting the provisioning of completely empty virtual servers. They only have the operating system. Therefore, all their content will belong to the customer. The CSP is not entitled to any rights.

- **Platform as a Service (PaaS).** In this case, in addition to the operating system, it usually incorporates a BB.DD., programming utilities, "web services", etc. All applications developed by the client with these programming tools, other applications that are added and the associated data, will be their property and will not generate any rights in favour of the CSP.

- **Software as a Service (SaaS).** In this case, the customer is limited to using an application or an integrated set of them in the Cloud. Therefore, only the content stored there will be their property: data, metadata, resource tagging and perhaps the scripts allowed for automation, among other possible uses.

By way of summary, this clause ensures that the service agreement never implies the transfer of any intellectual property rights in favour of the CSP, which must undertake not to process, transfer or provide access to the client's content to third parties, either in part or in full, in any form or by any means whatsoever.

1.1.2.8 Limitation of liability

In reviewing their respective contractual obligations, the parties (CSP and customer) should protect those that represent a significant risk to them, by including in this section economic remedy clauses or obligations to indemnify in case of non-compliance by the other party with its contractual obligations, or if deviations in the level of service occur.

If this is not possible, at least the standard clauses that the CSP has included in its contract and that normally exempt or limit its liability should be carefully reviewed and assessed.

In general, except for those matters that may be beyond the control or will of the service provider, the CSP should be liable to the customer for any damages that may arise as a result of entering into the contract for the provision of Cloud services.

1.1.2.9 Transfer of control

This clause foresees a situation of change of control in the CSP, e.g. due to a takeover, takeover or merger. It could be drafted in such a way that, in such a case, the new operator that will offer the contracted services in the Cloud is obliged to inherit the current contractual conditions, or the customer has the power to terminate the contract.

However, voluntary termination or termination of the service agreement, perhaps by the CSC, should also be provided for in a similar way to this clause.

1.1.2.10 Subcontracting chain

In the event that we are contracting an application in the Cloud, SaaS type, it may be the case that we do so with an independent software provider ("software house" or software developer) and the latter does not have virtual infrastructure and must outsource it. If this is the case, the Data Processor Agreement (signed by the client company and the SaaS provider) must state that the Data Processor (the SaaS provider) subcontracts the services to an IaaS or PaaS provider, indicating the name of the subcontracted company (the CSP where the data will be stored). Thus, a chain of subcontracting with other third parties may occur. It represents a successive performance of on-demand processing, where one of the providers providing the service may be located outside the EU territory, in one of the so-called third countries.

Annex 1. Contractual clauses and cloud computing

In order for the subcontracting of services in a service chain to be legitimate and in accordance with European law (especially Data Protection law), the customer acting as the Controller is obliged to require the execution of a contract of processing on behalf of the Controller, where it is stipulated that the service provider (Processor) will only act on the instructions of the Controller who is the subject of the service. If the service provider is also located in a third country, it is necessary to verify that this country is covered by an adequacy decision of the European Commission.

By means of the contract of processing on behalf of a Controller or "Processor", as provided for in art. 28 of the GDPR, a Controller established in the EU successively transmits to the various CSPs involved, the commitment regarding the conditions and guarantees that they must provide to ensure the level of protection of personal data, appropriate to the provisions of the GDPR.

In addition, any service provider that is part of the cloud outsourcing chain must provide sufficient guarantees regarding the technical and organisational security measures for the personal data covered by the service. They must be protected against erasure, alteration, unauthorised disclosure or access and against any other unlawful processing of personal data.

Article 28 of the GDPR states not only the need for a processor contract, stating *"3. Processing by the processor shall be governed by a contract or other legal act under Union or Member State law, which binds the processor to the controller and sets out the subject matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller"*, but also states *"2. In the latter case, the processor shall inform the controller of any intended change in the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes"*. Paragraph 3 of the same Article details the minimum content of such a contract.

In addition, this contract for processing on behalf of the CSP should include a commitment to formalise this type of agreement with all third parties involved in the provision of the service and so on, informing the CSP immediately if any changes to these agreements are foreseen.

1.1.2.11 Early termination for non-compliance with SLAs or even freely

This clause protects the customer against the CSP in the event of a degradation or breach of the service level (SLA) expected and contracted by the customer. It is advisable for the customer to protect himself by providing for a possible termination of the contract for such causes, regardless of any indemnity agreements.

Provision should also be made for the cancellation or termination of the contract for any other circumstances, such as the intention to migrate to another CSP offering better conditions to the customer.

The ownership of the information and other applications that the customer has placed in the CLOUD must be made clear (see Intellectual Property clause).

An orderly return of information should be agreed, ideally establishing a standard format for the data, with a transitional period to enable timely migration of data and applications to another CSP or, where appropriate, to a local DPC. This end-of-service process should provide for and detail an exchange format, which makes extraction feasible without compromising the integrity of the data. It would be useful if the CSP were contractually obliged to cooperate in the framework of a data migration to the new infrastructure specified by the customer. If possible, this should be free of charge.

Once the data is replicated in its new location, a secure deletion process must be ensured at the leaving CSP, which eliminates any possible subsequent security breach. Such a future situation, when the contractual relationship between the customer and the CSP ceases to be in force, cannot in any way compromise the responsibility for the data. Attention should be paid to possible legislation obliging the provider to retain data for a certain period of time after the end of the relationship.

It is always advisable for the customer to have a clause in the contract that allows him to terminate the contract without giving a reason by giving reasonable and agreed notice. This provision is relevant in contracts that are based on the provision of services based on technology, which, although of no interest to the CSP, has a crucial influence on the customer. No one can guarantee that a leading supplier today will still be a leading supplier in several years' time. If such a clause is not accepted by the CSP, at least any penalty or demand for full payment of the service in case of unilateral early termination should be identified in the general terms and conditions.

1.1.2.12 Service Level Agreements

Service Level Agreements (SLAs) rather than a contractual clause are usually an addendum to the contract or a specific document.

The service level cannot be managed if an SLA has not been previously subscribed with the CSP, just as it cannot be subscribed if the customer of the service has not previously defined its Service Level Requirements (SLR). In case a standard SLA of the CSP is subscribed, the customer must also verify that it meets its SLR requirements.

The National Institute of Standards and Technology (NIST) defines a Service Level Agreement as: "An SLA represents the understanding between the customer and the CSP about the expected level of service to be delivered and, in the event that the provider fails to deliver that service at the specified level, the compensation available to the customer".

Some CSPs already provide for the monitoring of SLA compliance through a standard set of indicators that can be consulted through a unified dashboard from the customer portal, or by sending regular reports to the customer by e-mail.

Once migrated to the Cloud, the customer has the responsibility to ensure that the terms of the SLA are being met and that key performance indicators (KPIs) are monitored. It will be the KPIs that accurately reflect ongoing performance. Once the customer has defined and developed KPI parameters, it can work with the CSP to create alerts when performance falls below an acceptable range. By analysing the cause, performance can be optimised on an ongoing basis.

It is advisable that, when contracting the cloud service, definitions of own or standard KPIs are already available. These can be added initially as an annex to the contract, which binds the CSP to compliance with the SLAs, based on tangible values. Non-compliance can lead to penalties agreed in the contract.

Remember that service level indicators must be specific, measurable, achievable and realistic.

IT "best practice" frameworks and standards, such as ITIL, define a comprehensive Service Level Management, which is good to consult prior to contracting.

1.1.2.13 Notification of incidents

This clause must clearly define the mechanisms for reporting incidents, especially security incidents, between the CSP and the customer. Specific interlocutors and forms of communication should be defined, in line with the security measure [op.nub.1] of Annex II of RD 311/2022 of 3rd May.

Special consideration should be given to defining the maximum time that may elapse from the occurrence or discovery of the incident until it is reliably reported. It is also important to define whether the customer will have access to consult by any means the logs, transactions and accesses that affect his own data environment.

In addition, provision may be made for financial or reputational costs incurred by the customer as a result of a CSP security incident, possible financial compensation and the appointment of a neutral arbitrator to assess this. It may be the case that, due to legal requirements, third parties must be notified by means of specific notifications, given that the customer acts as Data Controller.

Centro Criptológico Nacional

ANIVERSARIO

CCN-CERT

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es