∞drive

Practical guide

CIOs, CISOs

How to make digital sovereignty a shield for your sensitive data

CIOs, CISOs

How to make digital sovereignty a shield for your sensitive data

Table of Contents

1

Digital sovereignty

A concept worth understanding

a) What does digital sovereignty mean?

Against a backdrop of growing dependence on digital giants, companies are increasingly aware of the need to **keep control of their data**, especially the most sensitive. This has led to the emergence of the concept of "digital sovereignty", designating the ability of organizations to be autonomous and independent in their use of digital services and data protection.

Implementing this **digital independence** means **adopting independent technological solutions that store data on French or European territory**.

These so-called "sovereign"solutions offer the highest guarantees of digital independence, and are protected against foreign interference. The concept of digital sovereignty has taken on particular importance with the meteoric rise of the cloud.

Digital sovereignty has become a strategic issue for organizations involved **in critical activities** and handling **sensitive data**, such as government agencies, vital operators, the healthcare sector, banks, insurance companies and industry.

The use of sovereign cloud solutions ensures that this strategic data is subject to local laws and regulations, and therefore cannot be captured by foreign powers relying on extraterritorial laws.

65%

of French executives and managers believe that digital sovereignty is a major issue for their company.

b) Why is digital sovereignty so important for companies handling sensitive data?

Gaining executive buy-in on the importance of digital sovereignty

Eminently strategic, the issues of digital sovereignty and protection against extraterritorial laws are strongly linked to corporate culture, and will not find the same echo within all structures. A defense manufacturer or a multinational will not be sensitive to the same arguments. And yet, every company has an interest in protecting its most sensitive data.

Strategic challenge: regaining control over data

Using the solutions offered by the web giants does not guarantee data confidentiality. In fact, they are subject to extraterritorial laws. This mechanism poses a threat to corporate interests. Regaining control over your data becomes crucial.

Ethical issues: creating trust

The quest for digital sovereignty also has an ethical dimension. The issue of data protection is particularly important in the European Union, which has some of the strictest legislation on the subject. For companies, the quest for digital independence becomes a question of differentiation and trust.

Business issues: safeguarding your business

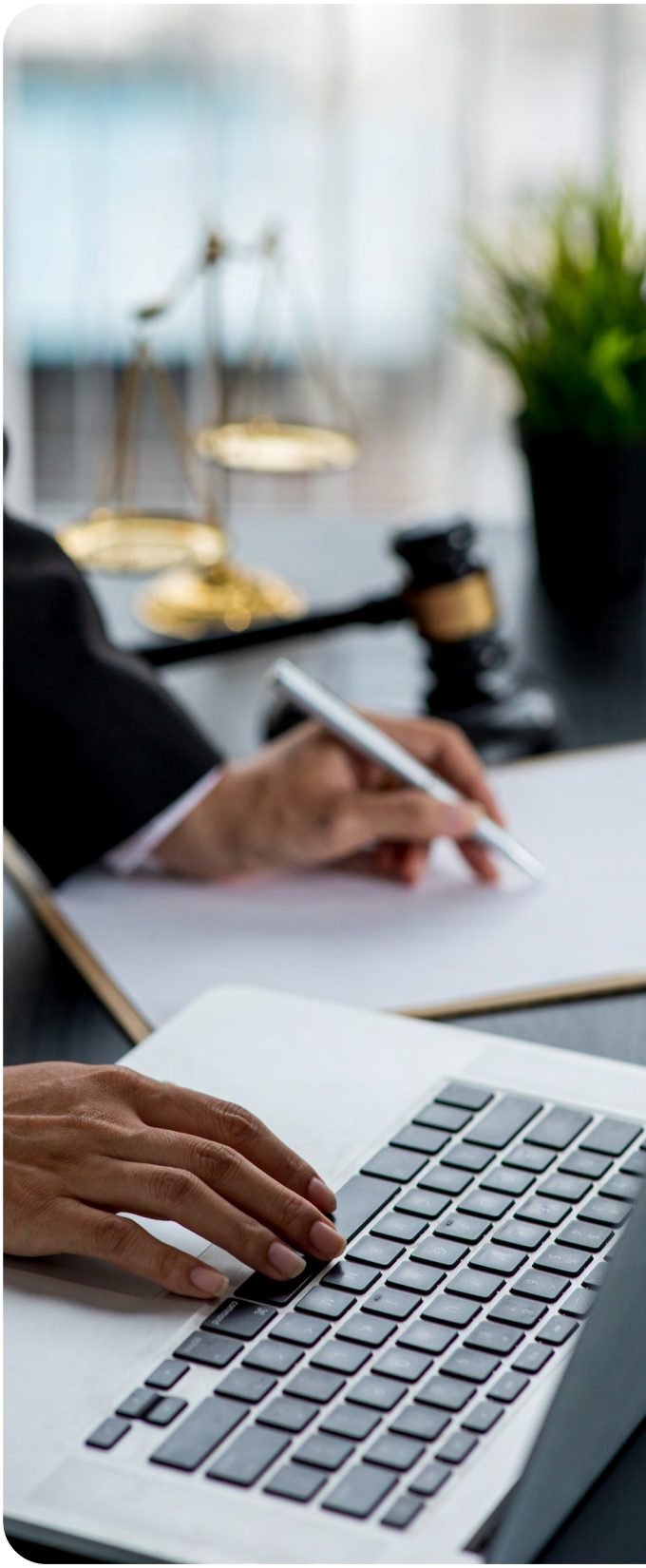
Protecting sensitive and strategic data is part and parcel of preserving knowledge and know-how. Today, data is a company's most precious asset, and it is in its interest to protect it from foreign interference.

c) Digital sovereignty as protection against extraterritorial laws

At a time when data produced in Europe is concentrated in the hands of web giants - all of whom are based outside the European Union's borders - digital sovereignty is of strategic importance.

U.S. legislation, for example, authorizes the country's government agencies to access data located in datacenters owned by U.S. companies, even if these datacenters are located abroad (in Europe, for example). All this without any procedure and without having to inform users. A situation that represents a major risk of data breach and industrial espionage. The extension of Section 702 of the Foreign Intelligence Surveillance Act (FISA) until 2026 is a case in point.

Digital sovereignty protects data from the risks of outside interference by putting it beyond the reach of extraterritorial laws.



d) How does Oodrive Work reconcile productivity, security and sovereignty?

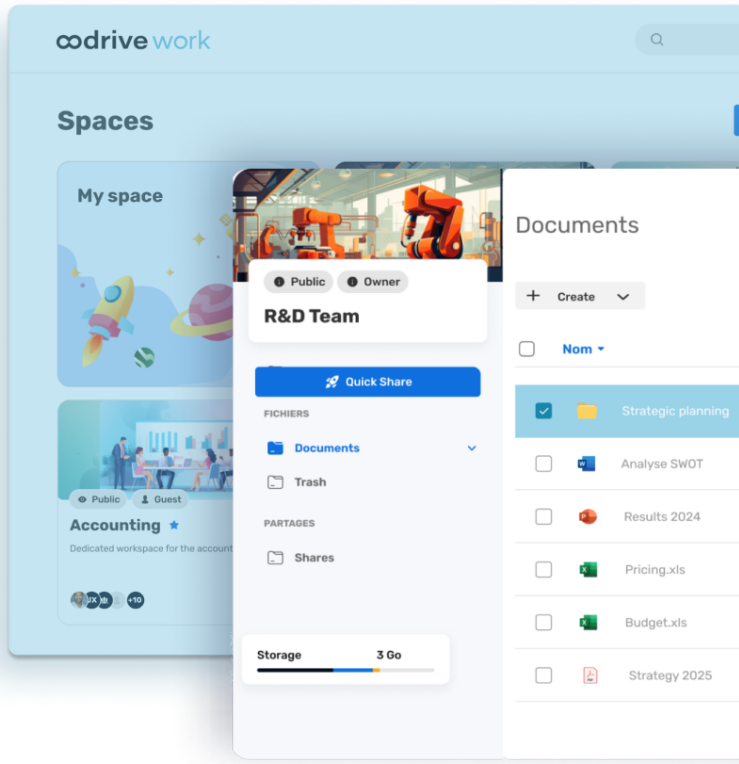
Oodrive Work is a highly secure collaboration solution that meets all sovereignty requirements. It relies on the most effective technologies and the most demanding certifications to protect data: SecNumCloud qualification, ISO 27001 and HDS (Health Data Hosting) certifications.

SecNumCloud is the ANSSI's security accreditation for the most demanding cloud solutions in terms of security and sovereignty.

An expert in the management of sensitive data, Oodrive is one of the major players in digital sovereignty on a European scale. Oodrive ensures that companies have complete control over their data, including when this data is shared internally and externally. Sensitive data is immune to extraterritorial laws.

With its intuitive, easy-to-use interface, Oodrive Work enables organizations to reconcile productivity, security and data sovereignty.

As a SaaS solution, Oodrive Work is backed by customized cloud hosting adapted to the criticality of companies' activities and the sensitivity of their data. Different hosting modes are available.



Public Cloud

Machines, servers and security components are shared. This solution is attractive for its ease of use and affordability.

Private Cloud

With this type of hosting, hardware resources and services are individualized.

On-premise

Companies deploy the solution directly on site (on their own machines and servers). It is then placed under the control of their own IT teams.

Regulatory compliance by design

Oodrive solutions comply with the most stringent regulations as soon as they come into force, thanks to *Security by Design*. We are in fact the first and only SaaS software publisher to be SecNumCloud qualified, thus benefiting from the highest degree of security delivered by ANSSI.

SecNumCloud
Qualified since 2019 by ANSSI

ISO 27701
Privacy protection standard

HDS
Certified For Health Data Hosting Level 6/6

NIS2
Directive to strengthen cybersecurity in the EU

DORA
General Data Protection Regulation

2

Case studies

3 companies that have strengthened their digital sovereignty

How can you ensure the digital sovereignty of your sensitive data? How can you collaborate effectively in a sovereign work environment? Answers to these questions from 3 companies and institutions using the Oodrive Work solution.

Use case 1 - French Ministry of Defense
Efficient collaboration on the move

MINISTÈRE DES ARMÉES

To meet the needs of the French Ministry of the Armed Forces for sharing sensitive files and working collaboratively in mobile mode, the DIRISI (Direction interarmées des réseaux d'infrastructure et des systèmes d'information) has deployed the Oodrive Work solution. Accessible on the move, the solution - dubbed *"Defense Drive"* - enables all types of files to be stored and shared via a simple link.

The benefits of Oodrive Work

- UAF-approved solution ("used by the French armed forces"), a label awarded by the French Ministry of the Armed Forces.
- Solution for storing and sharing large files (no size limit).
- Versatility of use and ease of use for users: collaboration, backup of smartphone media (videos, photos), synchronization of work directories.

Use case 2 - Arquus

Complying with regulations on restricted data without hampering productivity

Military equipment manufacturer Arquus designs, delivers and deploys high-performance armored vehicles worldwide, with the French army as its first customer. Data is classified on four different levels, depending on its sensitivity: restricted, classified, secret and top secret.

Arquus wanted to build a working environment that fully complied with the regulations governing the processing of restricted data, while at the same time streamlining exchanges between its 2,000 employees. The chosen solution therefore had to integrate with Microsoft Office 365, the suite used by the company, all with ANSSI-certified security. The challenge was met with the creation of a separate, secure and autonomous on-site network: the *"Arquus Defense Network"*, an environment dedicated to data referred to as *"restricted"* by French regulations.

> *"We want the user experience on restricted data to be as close as possible to that of our other systems. The solutions must meet increasingly stringent regulations, while being as easy to use as the usual tools."*
>
> **Yannick Lestriez**
> CISO & Infrastructure Manager - Arquus

Arquus also uses Oodrive Work as a secure SaaS platform to exchange data with its partners and customers, including contracts and calls for tender. Setting up an external collaboration tool like Oodrive Work, which is simple to deploy and use, takes just one day.

The benefits of Oodrive Work

- Secure, ANSSI-qualified solution, approved by the defense services.
- Solution implemented in 24 hours.
- Users collaborate without friction or frustration, without slowing down their productivity, using the usual Microsoft 365 interface deployed on the Oodrive infrastructure.

Use case 3 - Paris Bar Association
Streamline and secure the exchange of sensitive documents

The Paris Bar Association, France's largest bar association with almost 35,000 lawyers, accounts for around 50% of all lawyers in France. With a particularly dense volume of business, the Paris Bar works with many confidential and sensitive documents, for example, in the context of major trials, and within the Bar's committees and Council.

The institution was looking for a sovereign solution to manage the secure sharing and exchange of its data. This solution had to facilitate and secure the various exchanges between lawyers, but also with the judicial administration (magistrates, clerks, etc.).

The Paris Bar chose Oodrive Work. The solution was quickly adopted and integrated into the lawyers' day-to-day work. For example, it enables documents to be communicated in real time to all those involved in a sensitive case. Around 250 members of the Paris Bar and more than 140 of their colleagues use Oodrive services on a daily basis.

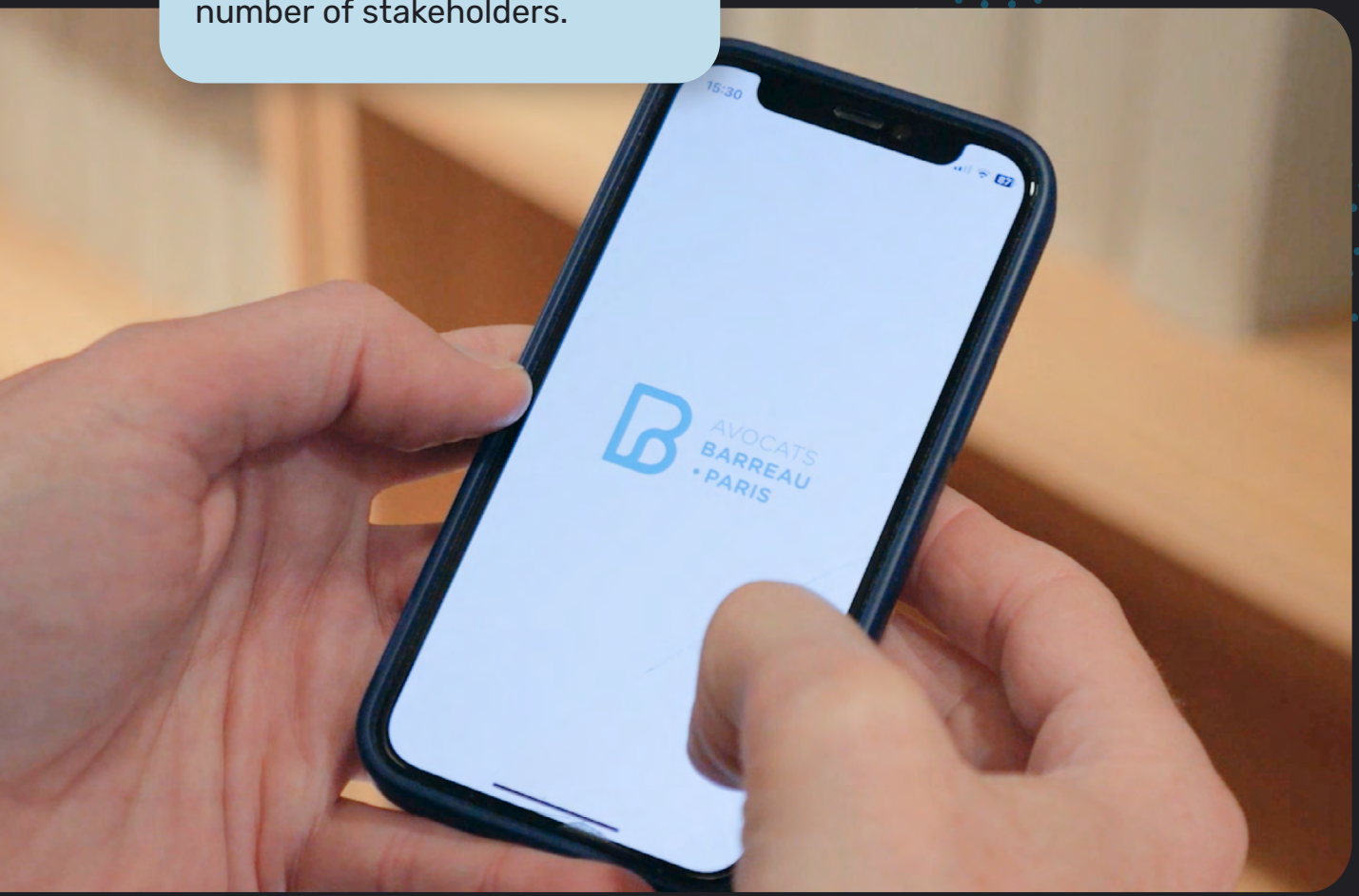
"The arrival of the RGPD led the Paris Bar to look for a solution that was both Franco-French, for reasons of territoriality, and validated by ANSSI, via its SecNumCloud label. Of the solutions studied, only Oodrive met these requirements. Lawyers have created real communities of sharing and collaboration."

Christophe Bacoup
CIO of the Paris Bar Association

The Paris Bar also uses Oodrive Meet to organize meetings of the Conseil de l'Ordre and the Commission Numérique in a secure, dematerialized way, from the management of invitations and votes to the minutes. Over a hundred people now use Oodrive Meet.

The benefits of Oodrive Work

- French solution validated by ANSSI's SecNumCloud label.
- Provides a secure, sovereign file storage and sharing service with no size limits.
- Efficient collaboration (ease of use, time savings) and confidentiality with a large number of stakeholders.



oodrive

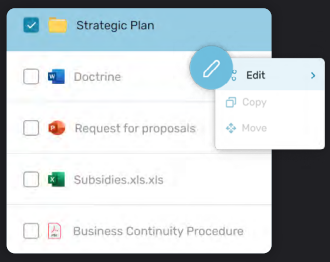
The secure, sovereign cloud collaboration suite

Qualified SecNumCloud since 2019 by ANSSI

Designed for private and public organizations, the Oodrive suite enables you to collaborate online in total security. With its four solutions on a secure European cloud, it guarantees the confidentiality, integrity and compliance of your sensitive data.

Trusted collaboration

oodrive work



- SecNumCloud-qualified collaboration suite
- Secure internal and external sharing
- Cyber-resilience
- Restricted Distribution

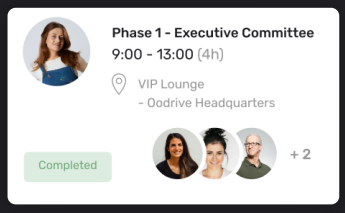
Electronic signature

oodrive sign

- Secure electronic signature
- Qualified electronic signature (QES)
- Electronic signature via API

Digitization of governance meetings

oodrive meet



- Management of governance meeting
- Unique Board Portal
- Secure Videoconferencing

Complies with regulations by design

NIS2, DORA, eIDAS... Oodrive solutions comply with the most stringent regulations as soon as they come into force, thanks to their Security by Design. In fact, we are the first and only SaaS software publisher to be SecNumCloud qualified, thus benefiting from the highest degree of security issued by ANSSI.

SecNumCloud
qualified since 2019 by ANSSI

ISO 27001, 27701
privacy protection standard

HDS
Certified Health Data Hosting Level 6/6

Sovereign Cloud
Oodrive is owned and operated in France

eIDAS
eIDAS compliant

NIS2
NIS 2 compliant

DORA
Compliant with DORA regulations

oodrive.com