ROCKET.CHAT · GUIDE · DIGITAL SOVEREIGNTY

Enabling digital sovereignty.

European public institutions are expected to take back control of their communications. They are also expected to work across agencies, Member States and partners that run different systems. This guide shows how to do both, without trading governance for reach.

THE SOVEREIGNTY TEST

Where does it run? | Who can access it? | Who can you reach? | Can you stay in control?



FOR THE EUROPEAN PUBLIC SECTOR · OCT 2026

rocket.chat

KEY TAKEAWAYS

What this guide covers.

Residency isn't sovereignty.
Data stored in the EU can still be reached under foreign law.

Sovereign can't mean isolated.
The Interoperable Europe Act makes cross-border interoperability a requirement.

Shadow IT starts where reach ends.
When the official tool can't reach a partner, people use whatever can.

You can test for it.
Nine checks show where your platform stands today.

CHAPTERS

01 Why sovereignty matters now p. 03
02 Sovereign doesn't mean isolated p. 05
03 The risk in everyday tools p. 06
04 What regulation asks for p. 07
05 Is your platform sovereign-ready? p. 08
06 Interoperable by design. Governed by you. p. 09
07 Who runs it today p. 11

rocket.chat

CHAPTER 01

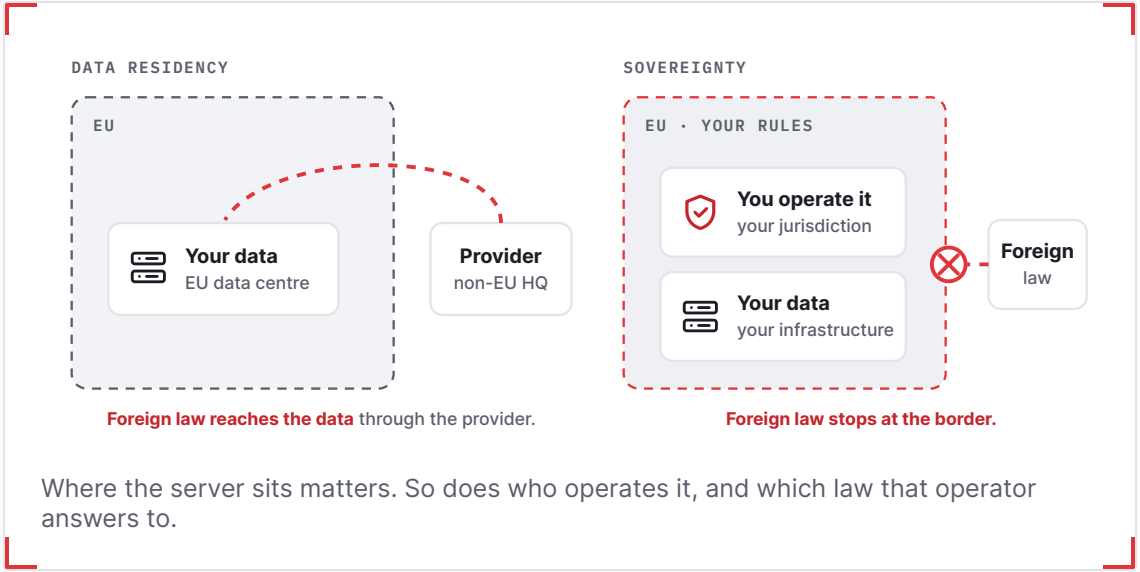
Why sovereignty matters now.

Government conversations carry citizen data, security decisions and policy before it is public. Whoever controls the platform those conversations run on controls who can reach them.

This is no longer hypothetical. In one widely reported case, US sanctions on the International Criminal Court's chief prosecutor in 2025 reportedly cut him off from his email, which ran on a US provider. A decision taken in one country reached the communications of an international institution in another.

Cases like this are one reason European governments are reducing their reliance on non-EU technology. France has announced it will move government computers from Windows to Linux, and the German state of Schleswig-Holstein is replacing Microsoft software across its administration with open-source alternatives.

For years, keeping data inside the EU looked like enough. It isn't. Where data is stored says nothing about who can be compelled to hand it over. A provider headquartered outside the EU can be ordered by its own government to produce data it holds, wherever the servers are. The U.S. CLOUD Act is the best-known example.



Where the server sits matters. So does who operates it, and which law that operator answers to.

Four questions decide it.

Sovereignty is the stronger test. It comes down to four questions about the platform your organization communicates on.

Where does it run?

On infrastructure you choose.

Under the law that applies to you, with no part of it depending on someone else's cloud.

Who can access it?

Only who your rules allow.

Checked on every request against your own identity system, and auditable afterwards.

Who can you reach?

Every partner you work with.

Other agencies, Member States and allies, whatever system they run.

Can you stay in control?

Leave a supplier, keep running.

Switch without losing your data, and keep working if a vendor's cloud goes down.

Residency is the starting point. Control is the destination.

CHAPTER 02

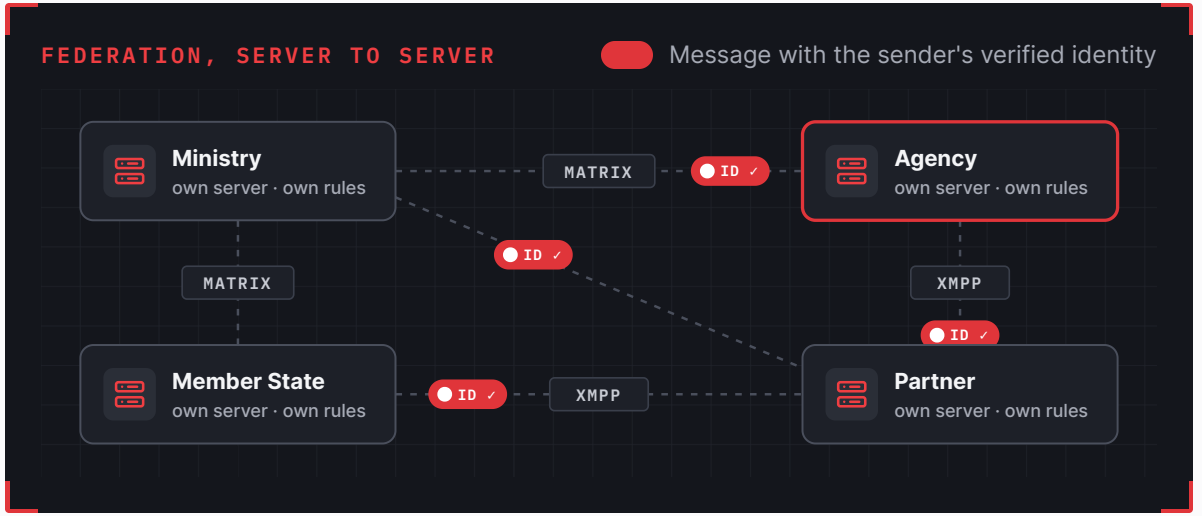
Sovereign doesn't mean isolated.

Public institutions rarely work alone. A ministry coordinates with its agencies, a city with regional authorities, an EU agency with every Member State. Each of them runs its own systems, and few run the same one.

That used to be an architecture decision. Under the Interoperable Europe Act, it is now a legal one.

This is where many sovereignty projects stall. Partners are asked to move onto the same platform, take a guest account, or connect through a bridge that loses track of who actually sent a message. Each of these trades governance for reach. Real interoperability lets every organization keep its own system, while identity, encryption and audit stay intact across the connection.

Federation makes that possible. Each organization keeps its own server, its own data and its own rules, and they connect over open standards such as Matrix and XMPP. Partners never have to adopt your system to work with you.



Sovereignty that can't reach a partner pushes people to tools that can.

CHAPTER 03

The risk in everyday tools.

Most public sector teams use a mix of chat, video and file-sharing tools, few of them designed for sovereignty. When the approved tool can't reach a partner, doesn't work on a phone or goes down in a crisis, people don't stop communicating. They move to whatever works.

Every one of these breaks the chain of custody. Information leaves the systems your organization governs, and no one can say afterwards who saw what. Shadow IT is what happens when the sanctioned tool can't reach the people it needs to reach.

Consumer messengers	WhatsApp, Signal or Telegram groups for operational work, with no record keeping, no access control and no audit. France, for example, has told government ministers and their offices to move off consumer messengers.
Foreign-hosted SaaS	Slack or Microsoft Teams used for sensitive work, on vendor-controlled public cloud subject to non-EU law.
Fragmentation	Each agency on a different tool, so cross-agency work moves to email and personal phones.
Legacy end of life	Skype for Business Server and Cisco Jabber are being retired. The vendor's path leads to public cloud, which sovereignty requirements often rule out.

CHAPTER 04

What regulation asks for.

European rules increasingly turn sovereignty from a preference into an obligation. Four frameworks shape most decisions in the public sector.

May 2018
GDPR
applies

Oct 2024
NIS2
national laws due

Jan 2025
Interoperable Europe Act
assessments begin

Sep 2025
EU Data Act
switching rules apply

Jan 2027
EU Data Act
switching charges end

GDPR

`Regulation (EU) 2016/679 · In force since 2018`

Personal data may only leave the EU under strict conditions, and controllers must be able to show where it goes and who can access it.

NIS2

`Directive (EU) 2022/2555 · Applies through national law`

Public administrations must manage cybersecurity risk across their supply chain, enforce access control and report significant incidents fast.

Interoperable Europe Act

`Regulation (EU) 2024/903 · Assessments since Jan 2025`

Public bodies must assess the interoperability of trans-European digital public services, and are encouraged to share open, reusable solutions.

EU Data Act

`Regulation (EU) 2023/2854 · Switching rules since Sep 2025`

Cloud and data-processing customers can switch provider and take their data with them. Switching charges end in January 2027.

NIS2 in particular expects access to be controlled and to hold up under audit. In practice, that points to Zero Trust: checking every request, not only the login.

The common thread is the four questions from chapter one. You must know where your communications run, who can access them, who they connect to and how you would leave a supplier. A platform you run yourself, federating over open standards, answers all four.

CHAPTER 05

Is your platform sovereign-ready?

Tick each statement that is true for the collaboration platform you use today. Each one means one more thing stays under your control.

Where does it run?

- [ ] We decide where the platform is hosted: on our own servers, in a sovereign cloud or air-gapped.
- [ ] No provider outside the EU can be compelled to hand over our data.

Who can access it?

- [ ] Access is checked on every request against our own identity system and our own rules, not only at login.
- [ ] We hold the encryption keys, and every action on the platform is auditable.

Who can you reach?

- [ ] We work with other agencies and partners on their own systems, without anyone having to switch to ours.
- [ ] When a message crosses to a partner, the sender's identity and the encryption stay intact.

Can you stay in control?

- [ ] The code is open to review, and we could switch supplier without losing our data.
- [ ] Communications keep running if a vendor's cloud or our internet connection goes down.
- [ ] Any AI runs on models we choose, inside our infrastructure, and acts only with our approval.

0–3 ticks

Exposed.

Your communications depend on decisions other people make. Start with where your platform runs, because that decides most of the rest.

4–8 ticks

Partly sovereign.

You control the core, but gaps remain, usually in how you reach partners or how you would leave a supplier. Those gaps are where shadow IT starts.

All 9 ticks

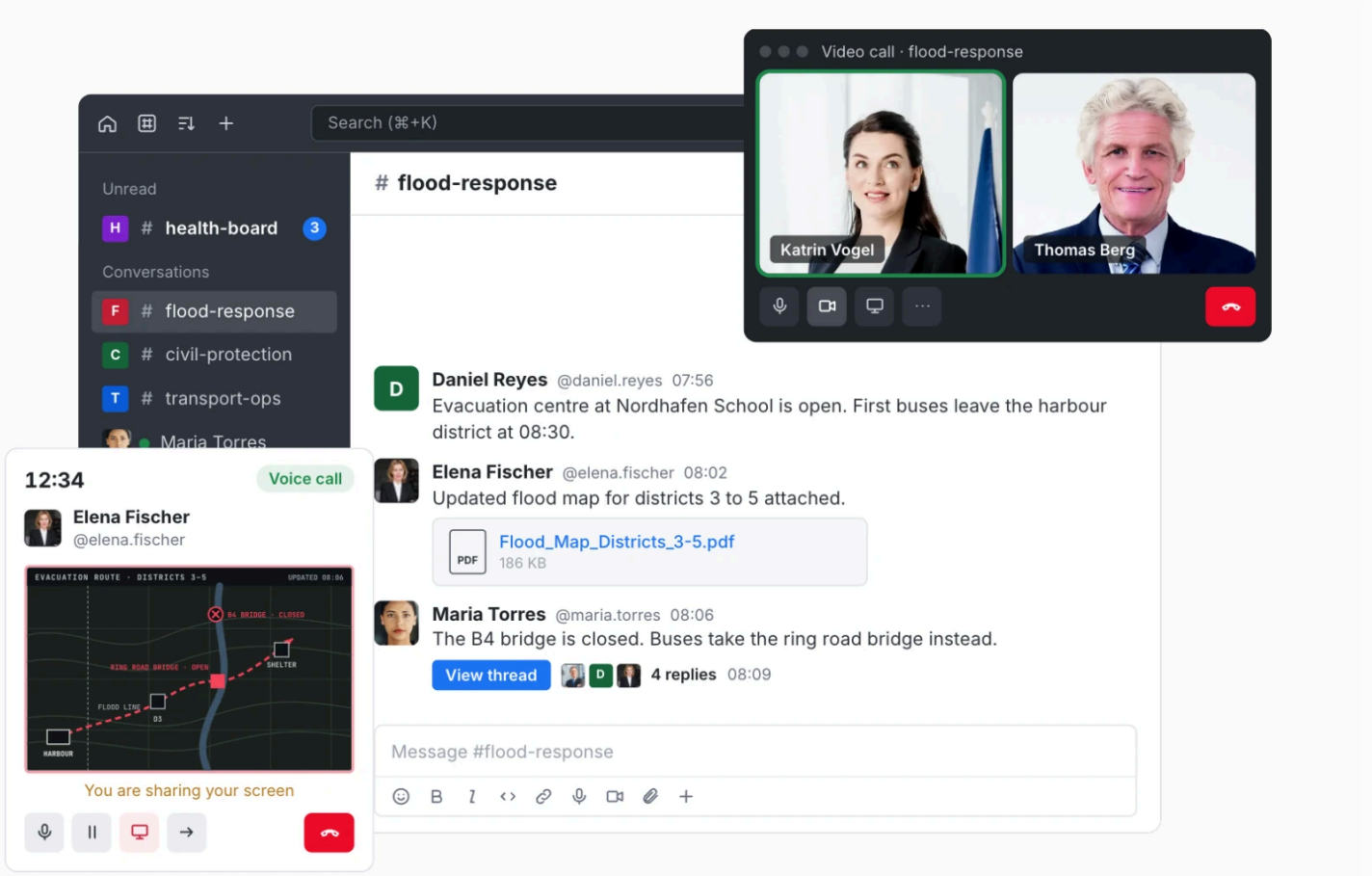
Sovereign-ready.

Your platform answers all four questions. Make sure it holds in practice, with real partners on their own systems.

Interoperable by design. Governed by you.

Rocket.Chat is the collaboration platform for organizations that must work across agencies, borders and partners. Chat, voice, video, file and screen sharing, apps and governed AI agents run in one platform, under one security model, deployed wherever you decide. It is trusted by public authorities across Europe.

Open source | ISO 27001 | SOC 2 Type II | Matrix + XMPP native



rocket.chat

Where does it run?

Deploy anywhere.

Self-hosted, air-gapped or in a sovereign cloud. Your data stays under your jurisdiction, never on someone else's cloud.

Who can access it?

Zero Trust, built in.

Attribute-based access control checks every request against your identity provider and your rules. End-to-end and post-quantum encryption protect sensitive work, and every action is auditable.

Who can you reach?

Native federation.

Native Matrix and XMPP federation, with no bridge in between, keeps identity and encryption intact across organizations. Where Microsoft Teams is in place, Rocket.Chat bridges it in and covers what Teams can't.

Can you stay in control?

Open and resilient.

Open source code you can inspect, and open APIs to connect your own systems. High availability and secure fallback channels keep you running through an outage, a cyberattack or a crisis.

YOUR JURISDICTION

Self-hosted
On your own servers

Air-gapped
Fully disconnected networks

Sovereign cloud
EU-operated infrastructure

Delivered with local partners

Rocket.Chat works with hosting and integration partners across Europe who deploy, run and support the platform close to you. Integrations and custom apps connect it to the tools your teams already use.

Map your four answers with our team.
We'll show you Rocket.Chat running the way your organization needs it, on your infrastructure.

Talk to sales →

rocket.chat

CHAPTER 07

Who runs it today.

European institutions already run their communications this way.



Real-time collaboration with Member States.

> “We were looking for a platform that's easy to use, secure, and hosted in the EU. Rocket.Chat delivered exactly that.”

Nadia Rosioru
Information Technology Officer, eu-LISA

The EU agency for large-scale IT systems runs Rocket.Chat in Germany, fully compliant with EU data protection law.

READ THE STORY →



Unified communications, live in two days.

> “Rocket.Chat met our communication needs: secure messaging, audio and video calls, and document sharing. It checked all the security and usability boxes for us.”

Jenny Nilsson
IT Strategist, Swedish National Electrical Safety Board

Hosted in the EU by a local partner.

READ THE STORY →

TAKE CONTROL

Ready to take control of your communications?

We'll help you test, deploy and run Rocket.Chat on your infrastructure, under your rules.

Talk to sales →