teamwire. | IONOS

Data sovereignty instead of digital dependency – Europe's wake-up call for IT decision-makers

A guide to the sovereign handling of sensitive data in times of global uncertainty

Preface

↓

Data sovereignty is not a nice-to-have. It is a necessity.

The world in which we conduct business, research, govern, and communicate is changing rapidly. With this change, the risks we face are also evolving. Global power blocs are not only vying for political or economic supremacy, but increasingly also for access to data. What seemed self-evident yesterday is now coming under pressure: namely control over who has access to confidential information, where it is stored, and under which legal system it is processed.

For companies, government agencies, operators of critical infrastructure, and organizations with security-critical tasks, this development is becoming an existential issue. Rising geopolitical tensions, laws like the US CLOUD Act, and our dependence on US tech giants show that digital sovereignty now impacts more than just IT setups. It affects security, resilience, and even strategic power.

As a provider of a secure communication platform that is used every day in sensitive application areas, we at Teamwire are experiencing the growing uncertainty of many decision-makers at first hand. The legitimate question is: How can I position my organization in a way that ensures absolute sovereignty and control over its data – and not third parties?

With this guide, we, together with our partner IONOS and other European solution providers, would like to contribute to raising awareness. Our aim is to provide guidance, make connections transparent, and outline concrete solutions.

Because the good news is Europe does not have its back against the wall. The necessary technologies, suitable partners, and regulatory frameworks, in many cases, are already in place. What matters now is the determined will to implement them.

Let us work together on a digital infrastructure that is not only efficient but also sovereign, secure, and sustainable. For an independent Europe. For full capacity for action at all times. For more control over our own data. And for the trust that our citizens, patients, and customers rightfully expect from us.

Yours,
Tobias Stepan

Tobias Stepan
Founder and Managing Director – Teamwire

0. Executive Summary

Data is at the heart of today's digital transformation, from everyday email communication to complex applications like artificial intelligence (AI). In this rapidly changing landscape, data is no longer just a byproduct of other processes. It has become a valuable economic asset and an independent resource. For companies, government agencies, and organizations with security-related tasks, this means: The question of where and how this data is processed and stored is no longer purely technical, but a crucial aspect of strategic sovereignty.

Together with IONOS and other trusted partners, we at Teamwire have created this guide to show how digital sovereignty can be implemented – safely, practically and in full compliance with the law. We share the belief that European values and technological independence must form the foundation for sustainable digitalization. With this guide, we aim to provide direction, offer new perspectives, and demonstrate solutions for achieving data sovereignty in practice.

Especially for operators of Critical Infrastructures (KRITIS), public safety agencies and emergency services (BOS), public administration, and healthcare facilities, digital self-determination is of vital importance. With the growing dependence on IT systems and platforms, there also comes significant dependency on corresponding providers – with many of them headquartered outside Europe. This dependency poses legal, technical, and economic risks that cannot be ignored. The question of data sovereignty therefore becomes a core issue of security, resilience, and innovation capability.

This guide is specifically aimed at decision-makers in security-critical areas and seeks to demonstrate how digital control can be regained and secured in the long term. It is not just about complying with legal regulations like the GDPR, but also about the ability to design digital infrastructures in a sovereign, secure, and sustainable way.

0.1 Objectives of the guide

This guide aims to foster a practical understanding of the risks and challenges around the use of non-European IT services while also providing concrete solutions for how digital sovereignty can be regained and strengthened.

The increasing dependence on non-European providers raises several questions. The guide describes the dangers associated with a lack of transparency, uncontrollable data transfers, and potential access by foreign authorities. Such scenarios are not hypothetical – they are relevant in practice. They pose a serious threat to data protection, compliance, reputation protection, and ultimately the innovation capability of the organizations involved.

At the same time, the guide aims to present concrete strategies for more digital self-determination. This includes, among other things, the development of transparent IT infrastructures, the integration of security and sovereignty aspects into decision-making processes, and the consistent evaluation of IT supply chains. A strategic shift to European IT providers can also make an important contribution to regaining digital control.

A special focus is placed on presenting European alternatives that are characterized by GDPR compliance, high performance, and clear legal frameworks. Solutions from Teamwire, IONOS, or other European partners exemplify a path towards greater data sovereignty. Furthermore, the guide references existing European initiatives and funding programs that can support organizations in building secure and sovereign infrastructures. Even though projects like the European data exchange platform Gaia-X have encountered significant hurdles in practice, they nevertheless highlight the strong political will to reduce Europe's digital dependency in the long term.

The guide is intended as a tool for decision-makers who want to not only meet regulatory requirements but, above all, design a sustainable, secure, and self-reliant IT landscape.

1. Introduction

The development of our digital world is a strategic paradox: Increasing digitalization promises efficiency, scalability, and innovation power – yet it simultaneously creates new dependencies, especially on non-European technology providers.

These dependencies rarely come without consequences – and it is precisely in this context that the term **data sovereignty** gains significance. But what does it mean to act digitally sovereign? What prerequisites must be in place? And where are there gaps in practice that could lead to risks?

“In key digital sectors, Europe is currently heavily dependent on non-European providers. According to the "Digital Dependence Index" (Konrad-Adenauer Foundation, 2023), Germany scores 0.82 on a scale from 0 (no dependency) to 1 (maximum dependency). A score of 0.75 is already considered critical. The EU as a whole averages 0.78.

Niklas von Tschirnhaus
Head of Consulting, People and Organizational Development – coac

1.1 Definition of data sovereignty

Data sovereignty describes the ability of organizations to exercise complete control over the use, processing, and storage of their data, without being dependent on third parties – particularly foreign states or providers. It can be divided into two main dimensions: legal and organizational.

Legal data sovereignty means that data is subject exclusively to the legal system of the country in which it was generated. In the European context, this means that data created in Europe should be governed exclusively by European law – in particular the General Data Protection Regulation (GDPR). At the same time, it should be protected from access by extraterritorial laws of other countries.

A prominent example of such laws is the **US CLOUD Act (Clarifying Lawful Overseas Use of Data Act)**. This U.S. law allows U.S. authorities to access data processed or stored by U.S. companies, even if that data is physically located outside the United States. Equally relevant is the **Foreign Intelligence Surveillance Act (FISA)**, which grants extensive surveillance powers to U.S. intelligence agencies over non-American individuals and companies. Both laws pose a direct threat to the data sovereignty of European companies and authorities if they use services from American providers.

Legal data sovereignty thus acts as a kind of shield against uncontrolled access by foreign intelligence services, law enforcement agencies, or private companies. It is not an optional aspect, but a prerequisite for legal certainty and trust in digital infrastructure.

Organizational data sovereignty extends this understanding of the term to include practical authority and control. It is not enough for data to formally be subject to European law. In addition, organizations must always know and be able to influence:

1. Where their data is stored,
2. Who has access to it, and
3. What it is used for.

To ensure this, technical measures such as **end-to-end encryption, Identity & Access Management (IAM)**, and controlled integration of external service providers are implemented:

Furthermore, the **definition and control of external service providers** is an essential aspect of data sovereignty. Only when it has clearly defined what services external partners provide, what data they are allowed to process, and what security requirements apply, can organizations maintain control over their digital processes.

These technical measures are complemented by organizational structures, such as regular audits, data protection-compliant contract design, and internal governance processes.

The aim of all this is **to establish a digital right to self-determination**, where organizations not only know where their data resides and who uses it, but also can decide for themselves which technologies, service providers, and standards they use to design their digital infrastructure. Data sovereignty is therefore much more than just a technical term – it is also a reflection of the ability to independently shape one's own digital future.

End-to-end encryption ensures that data, both during transmission and while stored, is only readable by the sender and the recipient. This not only protects against unauthorized access by third parties but also against state surveillance in third countries or unwanted access by the operator itself. However important and effective E2E encryption may be, it is not a cure-all. True data sovereignty requires more than just securing content. Why this form of encryption alone is not enough will be explained in Section 4 of this guide.

Identity & Access Management (IAM), in turn, enables organizations to precisely control and monitor access to data and systems. It defines **who can access which information, at what time**, and for what purpose, while ensuring transparency and traceability through centralized role and rights management.

> “Digital sovereignty begins where trust does not need to be imported.

Dr. Lars Nuschke
Senior Partnership Manager – Skribble

1.2 Differentiation of data residency, data localization, data protection, and data security

In the context of digital strategies, terms like data residency, data localization, data protection, and data security are often used interchangeably or mixed together. However, a clear distinction is crucial to correctly understand and implement data sovereignty.

Data residency refers to the physical location where data is stored – for example, a data center in Germany or the EU. Many providers advertise with "data storage in Germany," implying legal compliance and security. However, physical storage alone is not sufficient if the operating company is subject to the legal system of a third country, as is the case with U.S. companies subject to the CLOUD Act.

Note:
Data residency only indicates **where** data is stored – not **who** has access to it. Companies from non-EU countries can access data stored in Germany if their national laws require it. This is often overlooked.

Data localization goes a step further: It means that data is not only stored within a certain country or legal jurisdiction, as with data residency, but also remains there. This is particularly relevant for personal data, where data protection regulations like the GDPR must be strictly adhered to. Nevertheless, pure localization can be deceptive. If the underlying software, infrastructure, or responsible personnel come from a third country, it results in only a semblance of sovereignty without actual control over the processes.

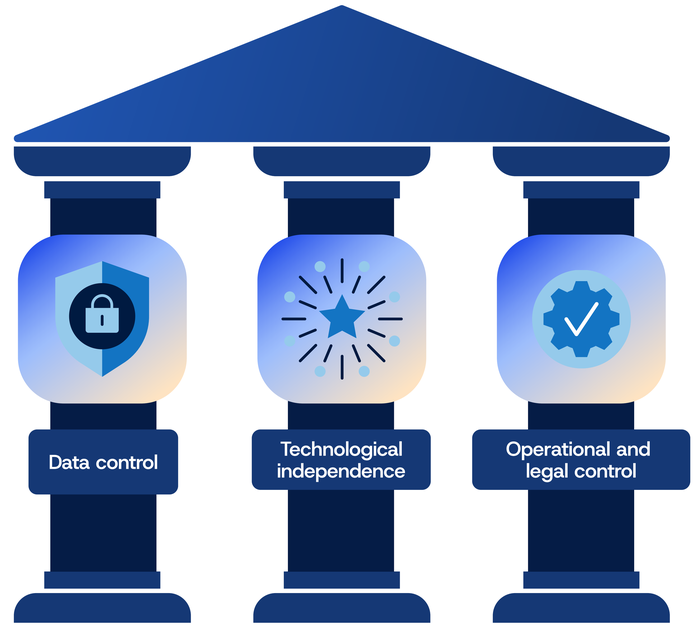
Data protection focuses solely on the protection of personal data. The GDPR requires European companies to process data lawfully, transparently, and purposefully, emphasizing the rights of the individuals concerned. Data protection is therefore a partial aspect of data sovereignty, but does not guarantee full control over digital processes.

Data security, on the other hand, focuses on technical protection against risks such as data loss, manipulation, unauthorized access, or system failures. It includes measures like firewalls, encryption, backup strategies, and the physical security of data centers. Again, data security is necessary but not a sufficient criterion.

Data sovereignty goes beyond all these concepts. It raises the question of who has complete control over technology, software, infrastructure, and contracts. Only when organizations are able to operate their digital systems independently, transparently, and reliably can true sovereignty be achieved. It is not enough to store data locally or implement a set of technical protection measures. What is crucial is that control over all relevant components lies in European hands.

1.3 The three pillars of digital sovereignty

Data control is an important part of digital sovereignty. Digital sovereignty itself is based on three pillars. Together they form the foundation for digital self-determination and they are: data control, technological independence, and operational and legal control.



The first pillar, **data control**, involves having oversight over the storage, use, and access to one's own data. It is the prerequisite for protecting sensitive information and complying with legal obligations.

The second pillar is **technological independence**. This means that companies and government agencies can rely on European, trustworthy technologies. The goal is also to avoid what is known as vendor lock-in, where an organization is permanently tied to a provider and thus loses its strategic capability to act.

The third pillar is **operational and legal control**. Organizations must be able to manage and control their digital processes themselves. This includes ensuring that the data is subject exclusively to European law, not jeopardized by extraterritorial laws or non-transparent contracts.

The three pillars together form the conceptual framework for our guide. They illustrate that data sovereignty is more than just an IT issue – it's a strategic domain!

2. Status quo: Digital dependency on US providers

The digital infrastructure of European organizations is largely based on products and services from major U.S. technology companies. These providers dominate key areas such as cloud computing, communication, office software, and collaboration.

Examples like Microsoft 365, Amazon Web Services (AWS), Meta/ WhatsApp, Slack, and Zoom illustrate how deeply U.S. software solutions are integrated into European IT daily life and the risks that arise from it. Let us take a closer look at three of the most widely used tools:

01

Microsoft 365

Microsoft 365 is one of the most widely used office and collaboration tools in public and enterprise-wide use. At the same time, it is a central focal point in discussions surrounding European data sovereignty. Although Microsoft operates data centers in the EU, the company remains subject to U.S. law. Various German data protection authorities, including the State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg, have expressed significant doubts about the GDPR compliance of Microsoft 365. A problematic element is the lack of transparency regarding which telemetry data is transmitted to Microsoft and whether complete protection against U.S. access can be ensured.

02

WhatsApp

Another example is WhatsApp, which is firmly established in the private sector but also used informally or – seemingly due to a lack of alternatives – officially in many government agencies and medical facilities. It is clear that as a subsidiary of Meta (formerly Facebook), WhatsApp processes metadata centrally in the U.S. While the service promises end-to-end encryption for content, the metadata, such as who communicated with whom and when, is accessible for analysis purposes. Legally, WhatsApp is required to disclose this data to government agencies upon request. Internal FBI documents even show that the data is delivered almost in real-time, approximately every 15 minutes.

03

Slack

Another commonly used tool is Slack, which is favored as a team communication platform, **especially in projects and interdisciplinary workgroups**. Slack is also owned by a U.S. provider (Salesforce) and thus stores data in a system that is not fully controllable under European law.

The GDPR-compliant use of Slack is theoretically possible in private sector companies by adhering to specific organizational, technical, and contractual measures but requires a sufficiently conscious approach to the software.

For critical sectors (critical infrastructure, authorities, public safety organizations, administration, healthcare), it is advisable to use data-sovereign, European alternatives with GDPR-compliant hosting and with no ties to the U.S.

These examples illustrate that **digital dependency on U.S. providers is profound and systemic**. The tools used are powerful and convenient, but at the same time, they are part of a digital ecosystem that offers European organizations limited control over their data and processes.

2.1 The legal situation: U.S. data laws with extraterritorial effect

The legal framework is a key factor in assessing digital dependencies. Many IT services that are widely used in Europe are subject to U.S., and not European, law.

CLOUD Act (Clarifying Lawful Overseas Use of Data Act)

The CLOUD Act, which came into effect in 2018, requires U.S. companies to provide data to American law enforcement authorities upon request – regardless of where the data is physically stored. This means that even if a cloud service provider operates its data centers exclusively in Europe, it can still be compelled to transfer data to U.S. authorities. This presents a fundamental contradiction to the European legal framework, especially the GDPR, which only permits such data transfers under strict conditions. The result is legal uncertainty for European users: despite local data storage, they cannot be certain that their data are truly subject to European data protection.

FISA (Foreign Intelligence Surveillance Act), particularly Section 702

FISA primarily allows U.S. intelligence agencies to monitor non-U.S. citizens' communications without a court order. Particularly relevant is Section 702, which permits access to communication data even if the servers are located in the EU – as long as a U.S. provider is involved. European users have no means of challenging this nor any effective legal protection.

USA PATRIOT Act & USA FREEDOM Act

The Patriot Act was enacted in 2001 following the September 11 terrorist attacks and grants U.S. authorities extensive powers to collect data abroad. Although it was partially replaced by the USA FREEDOM Act in 2015, which introduced some control mechanisms, many surveillance powers remain in place. What is particularly problematic is that affected individuals are generally not informed when their data has been requested or stored. For European organizations, this means they cannot reliably determine if and when their data is being accessed by U.S. authorities. This undermines the principle of transparency.

PCLOB (Privacy and Civil Liberties Oversight Board)

The PCLOB is a U.S. board that is meant to review the impact of security laws on privacy. In practice, however, it lacks legally binding powers, and its recommendations are not mandatory. During President Donald J. Trump's second term, the board was also weakened in personnel and largely rendered ineffective.

Executive Order 12333

This order from 1981 allows U.S. intelligence agencies to extensively collect information abroad, once again without judicial oversight and outside of traditional law enforcement processes. Among other things, it regulates how data from international communication carriers can be intercepted during transit. Since many transatlantic connections are technically routed through the U.S. or involve U.S. service providers, access under this order is often possible. Of particular concern is that this form of surveillance is conducted covertly and without notifying those affected.

The legal situation makes it clear that even if European companies and government agencies deliberately choose data centers in the EU, when using U.S.-based services, they remain subject to a foreign, uncontrollable legal framework. This leads to significant compliance risks, especially regarding sensitive data from the healthcare sector, public administration, or critical infrastructure.

3. Risks of digital dependency for European companies

In view of the legal situation described and the structural dominance of American providers, it becomes clear that concrete dangers arise for European organizations. Continued use of non-European IT solutions, particularly for institutions in critical infrastructure sectors, public administration, healthcare, and public safety organizations, poses not only a legal but also an operational and strategic risk. The following sections outline the key dangers that result from this dependency.

3.1 Data protection violations due to data access by U.S. authorities

The General Data Protection Regulation requires that personal data of European citizens be processed only within a legally secure framework. In particular, this means that access by unauthorized third parties, including foreign authorities, must be excluded.

This is precisely where the structural problem lies in using U.S.-based providers. The legal situation in the U.S. requires American companies to grant access to stored data when ordered by U.S. authorities – even if the servers are physically located in Europe. This provides extensive access possibilities for U.S. intelligence and investigative agencies.

For particularly sensitive sectors, such dependency has serious consequences that can undermine the public's trust in the integrity of state and medical institutions:

- Under the GDPR, patient data, medical records, and research information may only be processed under strictly controlled conditions. Covert access by foreign entities constitutes a flagrant violation.
- In public safety and emergency services (BOS) applications, deployment or radio protocols and situational reports could be affected. These are highly sensitive pieces of information with security-relevant content.
- In the energy sector, network control data or maintenance documentation could be affected, representing a potential vulnerability for attacks or espionage.
- In the public sector, confidential session documents, internal communication, or citizen inquiries could be affected. If such information falls into the hands of third parties in an uncontrolled manner, it poses political and diplomatic risks and can damage trust in the ability of government institutions to act.

3.2 Issues with certifications and audits

For many organizations, especially those in the public or security-related sectors, IT certifications are essential. Standards such as ISO/IEC 27001, BSI IT-Grundschutz , industry-specific norms (e.g., in medical technology or the energy sector), or sectoral compliance requirements (e.g., for police authorities or utility companies) set clear demands on data processing.

Key evaluation criteria include, among others:

- complete traceability of data flows,
- technical and organizational control over the IT systems,
- the use of trustworthy IT service providers whose contracts and supply chains are verifiable.

With prominent US providers, these requirements often reach their limits. The exact location of the data, the manner of its processing, and access by third parties often cannot be adequately documented. As a result, organizations risk losing existing certifications or having new audit procedures denied. This can also have an impact on eligibility for funding or bidding approvals.

> When building an Information Security Management System (ISMS) according to ISO 27001, it is advisable to examine at an early stage which data and processes in the company are particularly critical for data sovereignty. This way, certification requirements can be implemented in a targeted and effective manner.

Daniel Manzer
Managing Director –
ND Concepts

3.3 Loss of competitive advantages due to foreign data access

Digitally stored information has long been a strategic asset. Whether it is internal process data, research results, business models, or technical network information, those who have access to this data can influence markets, circumvent patents, or prepare targeted attacks.

A loss of data control therefore directly leads to a competitive disadvantage:

- In the medical field, research data on new therapies or medications can leak, resulting in innovations being utilized in third countries before they are applied in Europe.
- In the security sector, structural information on tactical operations, personnel deployment, or equipment standards can be deduced, providing potential attackers with valuable insights.
- In the energy and utility industry, it is network technical data that provides information about vulnerabilities, load, or resilience – with potentially critical consequences if exploited.
- In the public sector or government, confidential information about legislative initiatives, administrative processes, or negotiations can fall into the wrong hands. This makes political positions, negotiation strategies, or decision-making processes prematurely discernible and susceptible to targeted subversion.

It should be noted that even metadata, such as who communicated with whom, when, through which systems, and how frequently, can be sufficient to draw critical conclusions about organizational structures and decision-making processes. In sensitive areas, therefore, protecting not only the content but also the communication patterns is crucial.

3.4 Dependency on license and pricing policies of foreign providers

An often underestimated risk factor lies in the economic control of IT systems. Many U.S. providers pursue an aggressive licensing and pricing policy, which they can enforce thanks to their market dominance.

Especially for public institutions, non-profit organizations, and other budget-constrained entities, this means:

- Cost increases can be implemented at short notice without direct alternatives being available.
- License models (e.g., subscription instead of one-time purchase) significantly alter budget planning.
- Technical lock-ins complicate or prevent switching to other systems, for example, through proprietary file formats.

In sum, this leads to planning uncertainty that affects not only the IT departments but can financially burden the entire organization.

3.5 Loss of control over digital processes

A key goal of digitally sovereign organizations is the ability to manage their processes and infrastructures independently. However, many US tools operate like a kind of black box: the exact data processing is not transparently traceable, and updates often occur without the users' ability to influence them.

For security-relevant organizations, this specifically means:

- Disruptions or outages cannot be analyzed or resolved without relying on the provider.
- In the event of a cyberattack or supply failure, no autonomous actions can be taken due to the absence of critical system information.
- There is a dependency on an external provider that is subject to foreign jurisdiction.

This loss of control is unacceptable, especially in situations where the ability to react quickly is crucial, such as in disaster relief, medical emergencies, or energy supply.

4. Why data security is more than just end-to-end encryption

In discussions on digital sovereignty, end-to-end encryption (E2EE) is frequently cited as synonymous with secure communication. E2EE is indeed an essential component of modern IT security, as it protects the contents of communication from unauthorized access both during transmission and on the end devices of those involved. However, this factor alone is not sufficient to ensure comprehensive data sovereignty.

A central weakness lies in the aforementioned metadata. Even if the content of a message is encrypted, information about who communicated with whom, when, and for how long often remains accessible. For security-relevant organizations like public safety entities or critical infrastructure operators, this metadata can become a risk factor. It allows for conclusions to be drawn about internal structures, communication habits, or deployment patterns.

Another aspect is the physical location of the servers and the respective operating model. An E2EE-based application whose servers are operated in the U.S. or whose parent company is subject to U.S. law remains under the influence of extraterritorial laws. Even if content is encrypted, data leakage can occur through infrastructure access or administrative interfaces. Encryption alone is therefore not a guarantee of complete security or legal independence.

Security must also be considered from an organizational perspective. This includes control over software updates, system configuration, identity and rights management, and the clear definition of internal responsibilities. The use of zero-trust architectures, where no user or system is deemed trustworthy by default, can help minimize security gaps and reduce the attack surface. This concept is gaining importance, particularly for sensitive areas like health data or operational protocols.

5. European solutions that are secure, sovereign, and GDPR-compliant

The preceding explanations have highlighted the risks of digital dependency on non-European IT providers. Data protection violations, loss of control, and geopolitical uncertainties threaten not only IT security but also the economic resilience of European companies and public institutions. For operators of critical infrastructure, authorities with security tasks, and healthcare facilities, the question of viable, sovereign alternatives is becoming increasingly pressing.

The good news is that these alternatives already exist – and there has never been a better time to make the switch than now.

5.1 Why is now the right time to make the switch?

> The geopolitical situation requires that Europe become self-sufficient and independent in all digital sectors in order to be protected from arbitrary actions and protectionism.

Sascha Roeder
Managing Director – LIVECODER

Several developments are currently driving a realignment of digital infrastructure in Europe. A central driver is the increasing regulatory pressure on organizations. The GDPR has become stricter in its application, with few exceptions or transition periods granted. At the same time, the NIS2 Directive (Network and Information Security Directive 2 of the EU), which is currently being transposed into national law, extends obligations for a wide range of additional industries. Besides classic critical infrastructure operators, now mid-sized companies, for example, in the healthcare or administration sectors, are coming into focus. They not only have to implement appropriate protective measures but also demonstrate how they secure their digital supply chains, which is hardly feasible with US services.

> In times of global crises, geopolitical tensions, and growing dependencies on non-European tech giants, now is the moment for Europe to confidently take responsibility. It is not just about economic independence but about protecting our democratic values, our data sovereignty, and our innovation. Right now, it is clear: Those who do not control their digital infrastructure themselves lose not only technologically but also politically and socially in influence. A sovereign Europe means control over our data, our systems, and our digital future. It means being resilient to cyber threats, supply chain issues, and external political agendas. The clock is ticking – and those who do not act today will remain dependent tomorrow.

Fabian Huber
Senior Technical Evangelist – dox42

In addition, there are further European legislative initiatives such as the Digital Markets Act and the Data Governance Act. Both aim to regulate dominant platforms more strictly and increase control over data flows in Europe. These legislative measures reflect a growing political awareness of the importance of digital sovereignty.

Another factor favoring a timely switch is the increasingly tense geopolitical environment. Donald J. Trump's renewed term brings significant uncertainties for transatlantic collaboration and could further undermine the fragile balance in data protection. Simultaneously, tensions between the EU and China as well as Russia are rising. Digital infrastructures are increasingly viewed as geopolitical power tools, as they can provide insights into strategically sensitive areas.

Against this backdrop, economic considerations also come to the forefront. Supply chain risks, such as those posed by political sanctions, highlight the vulnerability of one-sided technology dependence. Especially in times of international instability, an independent European IT landscape gains importance. It not only protects against external access but also provides long-term planning security.

5.2 European alternatives

The often-quoted excuse that there are no powerful European alternatives to US tools is outdated. On the contrary, companies like Teamwire and IONOS demonstrate that functionality, security, and legal compliance can indeed be combined – without compromising user-friendliness or scalability.

teamwire.

An example of this is Teamwire, a messaging service tailored for professional use, with headquarters and hosting in Germany. Teamwire was specifically designed for public authorities, public safety agencies and emergency services (BOS), critical infrastructure (KRITIS) companies, and the healthcare sector and meets the highest security standards. The application is GDPR-compliant and implements modern protection mechanisms such as full encryption, a zero-trust architecture, and a customizable rights and roles system. Unlike U.S. services such as WhatsApp or Slack, no metadata is shared with third parties. Additionally, the application can be fully integrated into existing IT governance structures.

IONOS

IONOS is the leading digitalization partner and trusted cloud enabler for small and medium-sized businesses (SMBs). The company serves over 6.4 million customers and has a presence in 18 markets across Europe and North America, with its services being accessible worldwide. Its web presence and productivity portfolio caters to all digitalization needs, providing domains, web hosting and website builders with AI capabilities, as well as eCommerce and online marketing tools. The company also offers cloud solutions for businesses looking to move their operations to the cloud as they expand and develop.

> By shifting workloads to companies that are fully subject to European law, and with no loopholes, a significant contribution can be made to Europe's digital sovereignty.

Boris Gromodka
Business Development – Kindermann

A number of other specialized providers complement the European ecosystem. As our partner Cinify aptly states, "The close cooperation with European partners not only strengthens our own solution but Europe's digital economy as a whole. This creates a robust counterbalance to other market-dominating platforms – and a real opportunity to unleash Europe's innovative power on equal terms." Here is a brief introduction to some of our partners:

Xitrust

XITRUST
THE ESIGNATURE COMPANY

"The digital signature is a central element for legally binding communication in the digital space. It guarantees not only the authenticity of a sender but also the integrity and authenticity of a document. In the European Union, the eIDAS regulation (Electronic Identification, Authentication and Trust Services) provides the legal framework for the use of electronic signatures. The MOXIS signature platform helps companies and administrations digitize their signature processes by providing an eIDAS- and ZertES-compliant, European-developed solution for simple and qualified electronic signatures that are independent, secure, and GDPR-compliant."

dox42

dox42

"dox42 offers powerful, flexible document generation, which can be integrated into existing systems (such as SAP, Microsoft 365, Dynamics, etc.) as a public cloud, on-premises, or in sovereign cloud environments."

Planet Solutions

PLANET has a worldwide unique and leading solution for image and handwriting recognition based on modern artificial intelligence.

LIVECODER

Livecoder

LIVECODER is a European video cloud solution for secure, high-quality video streaming, full EU data sovereignty and compliance – plus interactive features for maximum engagement. Whether live or on-demand streaming: LIVECODER ensures perfect performance – flexibly as SaaS or BYOL in your infrastructure.

CASERIS

caseris

CASERIS makes a significant contribution to data sovereignty with TIMIO.360, a "modular communication platform for contact centers, customer service, and internal communication. TIMIO.360 is provided via IONOS's sovereign cloud infrastructure – it is GDPR-compliant, in German data centers and certified to the highest security standards. For KRITIS operators and public institutions, this means modern omnichannel communication, AI-based automation, and full data control – without compromising compliance or future viability."

Kindermann.de

Kindermann®

Kindermann.de: Kindermann.de is a manufacturer of modern conference and media technology with a strong focus on security. It supports sovereign hybrid communication in the public sector, without routing data through foreign platforms.

IndustryFusion X

IndustryFusion-X
DataSpace for Industry 4.0

"IndustryFusion-X follows an open, technology-agnostic, and transparent approach with its open-source framework, realized together with partners like IONOS. In combination with IndustryFusion-X's community-driven development, it creates a solid bridge between technical excellence, economic scalability, and political objectives."

coac

coac offers, among other things, SAIFTY, "a platform that uses AI to unlock unstructured data sources such as safety data sheets, regulatory texts, or technical documentation and generates structured, analyzable information. The platform offers ready-made reporting formats for CSRD and ESPR and can be directly integrated into existing business processes. SAIFTY is operated on European cloud infrastructure, e.g., IONOS Cloud."

Cinify

Cinify offers an all-in-one platform for digitalization in healthcare.

Skribble

Skribble is a cloud solution for legally compliant electronic signatures. Skribble supports simple electronic signatures, advanced electronic signatures and qualified electronic signatures in accordance with European law (eIDAS) and Swiss law (ZertES). By working with qualified identification partners and trust service providers, Skribble enables its customers to sign documents easily and securely online.

ND Concepts

ND Concepts helps companies build, operate and continuously improve professional management systems for information security, data protection and artificial intelligence. They focus primarily on ISO 27001, supplemented by ISO 27701 and ISO 42001.

nedyx Software

"At nedyx, we consciously rely on European infrastructures like the IONOS Cloud to provide our customers with a modern low-code platform that is secure, high-performance, and fully GDPR-compliant."

Aretek

Aretek was founded in 2015 to support the distribution of security products in Italy. We have extensive experience as a reseller in the industry and are able to support other resellers both technically and sales-wise. Aretek currently distributes the following brands: AnyDesk, Teamwire, Impossible Cloud, Splashtop, Nanosystems, Comet Backup, SafeDNS, Avast, and G DATA. DMarc.AI has recently been added to the list of distributed brands. Aretek offers innovative products that strike a balance between cost and performance and currently has a network of over 1,200 partners.

ISEC7

In times of growing geopolitical uncertainty, data sovereignty, secure communication and digital resilience are becoming increasingly important – for companies, public authorities and especially for security institutions and operators of critical infrastructure. The ISEC7 Group offers customized software solutions and services that meet these requirements – compliant, mission-critical and field-tested. With a focus on managed mobility and the digital workplace, ISEC7 helps its customers to act with confidence even in critical situations.

Today, the alternatives are technically mature, legally secure, and economically attractive. By switching early, organizations not only reduce their risks but also actively strengthen the digital independence of their own organization, and ultimately the sovereignty of Europe.

6. Strategies for IT decision-makers

Ensuring digital sovereignty is no longer just an academic issue, but a strategic imperative. For businesses, government agencies, and organizations with critical tasks, it is a prerequisite for IT security, data protection, and long-term competitiveness. While it was previously believed that European solutions were functionally inferior or not widely adopted, a different picture is emerging today: European providers offer technologically equivalent, often even more flexible and better-integrated, solutions that fully meet the requirements for compliance and security.

Against this backdrop, it is up to IT decision-makers to act consciously. The transition to sovereign IT structures does not need to be rushed but should be strategically planned and deliberately implemented. A gradual approach is particularly recommended, starting with the areas where the risk is highest: internal communication, document exchange, and the storage and processing of sensitive data.

6.1 Concrete recommendations: How to successfully transition

The path to greater digital self-determination is not a short-term measure but a long-term process of transformation. A successful transition to sovereign IT begins with an honest analysis of the current situation. First, all deployed tools, cloud services, and communication platforms should be systematically recorded and evaluated – particularly in terms of their origin, legal status, and technical transparency.

A second, crucial step is risk assessment. Which applications are security-critical? Where are potential GDPR violations or compliance risks? Where, in the worst-case scenario, is there a risk of losing control over systems and data? In sectors such as critical infrastructure (KRITIS), transitioning to European solutions is particularly urgent, as confirmed by CASERIS:

> Critical infrastructures – from healthcare to energy supply – are the backbone of our society. Their functionality determines safety, stability, and the public's trust. Especially in these areas, it is essential that digital systems are not only highly available and efficient but also trustworthy and operated with sovereignty. A lack of control over data flows and non-European legal access leads to a highly unpredictable risk – with potential impact on security, compliance, and crisis response capabilities.

Pascal Porath
Marketing Director – CASERIS

Parallel to the risk assessment, a targeted evaluation of suitable European alternatives is recommended. This should not be based solely on functionality comparisons but should also include organizational and legal aspects:

- Can the provider guarantee GDPR compliance?
- Is the data flow auditable?
- Can technical security concepts like Zero Trust or full encryption be implemented?

Services like Teamwire for messaging or IONOS for cloud infrastructure are proven providers that are already in use in security-sensitive environments.

Another key success factor is early involvement in new projects. Sovereignty should be understood as an integral part of digital strategy. This also means further developing the organization's IT governance: for example, by establishing clear processes for provider evaluation, transparent contract design, regular audits, and consistent access management.

7. Opportunities through sovereignty

The digital sovereignty of European organizations not only provides protection from risks but also opens up a wide range of strategic opportunities.

A key benefit of sovereign IT structures is trust. As data becomes the most valuable asset for many companies and public institutions due to increasing digitalization, responsible management of this data is increasingly becoming a relevant factor. Citizens and patients, as well as business partners and regulatory authorities, expect that personal and business-related data does not enter foreign legal jurisdictions in an uncontrollable manner or be processed by third parties without adequate protection. By opting for transparent and privacy-compliant technologies, organizations send a clear message: Data protection is a priority.

Moreover, digital sovereignty offers the opportunity to gradually become independent of non-European technology providers. The relevance of extraterritorial US laws such as the CLOUD Act or FISA clearly demonstrates how high the dependence of European companies on uncontrollable legal frameworks can be. Sovereignty here means consciously avoiding one-sided dependencies and lock-in effects. Those who establish sovereign solutions today preserve the freedom to respond flexibly to new developments.

In terms of innovation, digital sovereignty also creates new opportunities.
When organizations have control over their technologies and data flows, space is created for tailor-made solutions. This is particularly advantageous in regulated sectors such as healthcare, energy, and public safety. This means instead of adapting standard solutions from overseas, organizations can develop and operate solutions that meet the specific needs and values of the European market.

Another crucial factor is legal and future-proof security. Companies and public authorities that rely on sovereign European solutions gain greater planning certainty regarding data protection compliance. They minimize the risk of sudden licensing changes, unforeseen price adjustments, or politically motivated export restrictions. Instead of adjusting to short-term market shifts and power imbalances, they can plan their IT strategy along stable, European guidelines.

> “Digital sovereignty is defining Europe's strategic resilience in the 21st century. It is reducing geopolitical dependencies, strengthening innovation capacity, and allowing us to shape technological progress in accordance with our ethical and legal values.

Olaf Classen
Cybersecurity Influencer

Finally, the consistent use of sovereign IT structures also contributes to strengthening the European technology ecosystem. Every contract awarded to a European company rather than a global tech giant strengthens local value creation, fosters innovation on the ground, and creates future-oriented jobs. European startups and medium-sized companies specializing in data protection and security solutions particularly benefit from this development.

In sum, data sovereignty is not just a protective mechanism — it also offers a range of advantages. It builds trust, ensures independence, fosters innovation, and strengthens the European economy. For IT decision-makers in critical infrastructures, public authorities, and the healthcare sector, this presents a clear course of action and a significant opportunity.

8. Solution in focus: Teamwire

At the heart of digital sovereignty lies the choice of trusted tools for daily communication. Messaging services, in particular, are an essential building block for many organizations. Teamwire offers a European solution that meets modern communication requirements while uncompromisingly focusing on data privacy, security, and legal compliance.

8.1 Why messaging platforms are particularly critical

In the context of digital sovereignty, messaging platforms play a particularly critical role. The reason lies in the high density of real-time information exchanged over these channels: personal data, deployment logs, medical information, situational reports, internal instructions. The constant availability and speed of such services increase the risk of data being shared in an uncontrollable manner or falling into the wrong hands. This is where the danger of a lack of data sovereignty becomes particularly apparent.

Many of the messaging tools currently in use are from US-based providers, such as WhatsApp, Microsoft Teams, or Slack. While some of these platforms feature end-to-end encryption, this alone is far from sufficient for data sovereignty. Even if the content of a message is encrypted, as mentioned earlier, metadata often remains accessible. And it cannot be emphasized enough: In many cases, this information alone is enough to draw compromising conclusions.

Moreover, platforms from third countries are often subject to extraterritorial laws. As outlined earlier, this means that US authorities may, under certain conditions, access data or metadata – regardless of where it is stored. For European authorities or organizations, this means that even with encrypted communication, there is a structural risk of data privacy violations. Full GDPR compliance is often not guaranteed under these circumstances.

8.2 Introducing Teamwire

Teamwire is a secure business messaging app developed in Germany, specifically designed for the needs of businesses, government agencies, and organizations with high security requirements. The core of the solution lies in user-friendliness, data privacy, information security, and maintaining digital sovereignty.

In contrast to traditional US-based tools, Teamwire is fully GDPR-compliant. The entire lifecycle of the platform – from server infrastructure with IONOS as a trusted partner to software development – is based in Europe. This means no dependencies on foreign law, no cloud access by third countries, and no legal grey areas. Teamwire also meets the requirements for encrypted communication, protects metadata consistently, and offers a powerful management layer for IT administrators.

Additionally, Teamwire is intuitive and easy to use. The app uses a user interface that is similar to common messaging apps but with added professional features. These include:

- Secure group communication with full encryption
- Zero-Trust security model
- Support for mobile devices and desktop clients
- Role and rights management
- Alert functions for emergencies
- Live location sharing (e.g., for emergency personnel)
- Push-to-talk communication (Walkie-Talkie function)
- Augmented reality features for mission extensions
- Broadcast messages for situational or crisis communication

For emergency services, disaster relief, hospitals, or energy providers, Teamwire offers a clear added value: a trusted platform that meets both technical and organizational requirements.

Comparison: Teamwire vs. US-Based Solutions

Feature	Teamwire	Microsoft Teams	WhatsApp	Slack
Server location	Germany/EU	Worldwide	USA	Worldwide, selectable
Data Sovereignty	100% EU data storage, no US reference	US law applies	US law applies	US law applies
GDPR Compliance	Fully	Limited	No	Limited
NIS-2 ready	Yes	Limited	Limited	Limited
Full encryption	Yes	Partial	End-to-End only	No
Control over metadata	Yes	No	No	No
Special functions for emergency and crisis communication	Yes	No	No	No
Dependence on Third Countries	No	High	High	High
Auditability and Transparency	High	Low	Very low	Low
Central user management and administration	Fully via admin portal	Via Microsoft 365 Admin Center	No	Plan dependent
On Premise/ Private cloud available	Yes	No	No	No
Industry specific certifications	ISO 27001, BSI C5	Partially	No	Limited

This comparison makes it clear: Anyone who wants to ensure confident, secure, and legally compliant communication cannot overlook a solution like Teamwire.

8.3 Use cases in public administration, public safety agencies and emergency services (BOS), energy and healthcare

The potential applications of a data-sovereign messaging platform like Teamwire span numerous security-relevant industries and institutions. Four key use cases illustrate the practical added value.

Public administration

In cities, municipalities, and ministries, digital communication plays a crucial role in daily administrative work. Teamwire enables the establishment of fully GDPR-compliant internal communication. The ability to create groups, securely exchange sensitive data, or send targeted alerts makes the solution ideal for government and municipal structures, such as in the city of Zirndorf and the city of Kleve. Thanks to the on-premises option, data-sensitive organizations can also host the software locally.

Energy sector

Critical infrastructure (KRITIS) businesses such as energy providers or network operators require reliable and secure communication channels. Teamwire enables fast, targeted communication with high availability and real-time capabilities. Features such as Push-to-Talk or broadcast messages are particularly useful for shift work and the control of complex systems. With full control over data flows, roles, and access rights, the service can be seamlessly integrated into existing security concepts.

Healthcare

In hospitals such as Landeskrankenhaus Andermarch, care facilities like Taurus Pflegeservice or emergency services, protecting highly sensitive personal data is paramount. At the same time, communication needs are extremely high. Coordinating emergencies, mobile visits, exchanging information with departments, or transmitting patient data now predominantly happens digitally. Teamwire provides a confidential and fully encrypted infrastructure that allows healthcare institutions to communicate quickly and securely on smartphones, tablets, and desktops. Compliance with GDPR is ensured, as is integration into existing hospital IT systems.

Public safety agencies and emergency services (BOS)

For police, fire services, and other emergency service units, fast, reliable, and most importantly, secure communication is crucial, especially during operations. With Teamwire, police officers like those from the Bavarian Police can exchange operational information in real-time. Centralized administration, as well as the ability to use the system in a protected on-premises operation, makes Teamwire the ideal solution for emergency service structures.

8.4 Advantages at a glance

- **100% GDPR-compliant & "Made and hosted in Germany":** All data is processed exclusively under German or European data protection laws.
- **Full data sovereignty and security:** No access by foreign authorities, no dependence on extraterritorial laws.
- **Easy-to-use much like consumer apps:** User-friendliness on the level of WhatsApp, without its data protection drawbacks.
- **Suitable for public authorities, BOS, health & KRITIS:** Tailored features for security-critical operational areas.
- **BSI-C5-certified hosting:** Available with public cloud, private cloud, or full on-premises operation.
- **ISO 27001:** The highest standard for protecting sensitive data and processes.

9. Conclusion

Data sovereignty is no longer just a theoretical or purely legal requirement – it has become a necessary foundation for businesses, government agencies, and organizations with sensitive infrastructures in Europe. In an increasingly interconnected and data-driven world, the level of digital independence directly determines competitiveness, innovation potential, and legal security. For critical infrastructure (KRITIS) operators, healthcare facilities, as well as authorities and agencies related to public safety, the protection of sensitive data is mandatory.

As this guide has shown, the use of US-based software and cloud solutions presents a real threat to the data sovereignty of European – and especially German – companies. Extraterritorial access laws undermine European data protection regulations. The result is uncertainty during audits and certifications, along with a continuous dependence on non-European market powers.

At the same time, European solutions like Teamwire demonstrate that there are promising alternatives today that are not only GDPR-compliant but also highly competitive in terms of functionality. Teamwire, for example, provides a secure, controllable communication platform specifically designed for sensitive applications like public administration, energy supply, and healthcare. The comprehensive features of the business messaging app show that digital sovereignty does not mean sacrificing user-friendliness or performance.

In short, transitioning to sovereign European IT solutions is technically feasible, economically sensible, and politically essential. It can be done gradually and will strengthen user trust in the process.

European data sovereignty thus provides the foundation for a self-determined, secure, and future-ready digital society.

> Europe's digital sovereignty is no longer an abstract vision, but an urgent necessity. Amid increasing geopolitical tensions and growing dependencies on non-European tech corporations, Europe's competitiveness is at stake.

Jan Vordenbäumen
Co-Founder and CEO – cinify

10. Next steps: From insight to implementation

This guide has shown that data sovereignty is essential for European organizations, particularly in critical infrastructures, public administration, and healthcare. However, between insight and implementation lies a multi-step process. Start today:

01 Schedule an obligation-free demo appointment: Take advantage of a highly practical demonstration of sovereign IT services. In an individual session, Teamwire will show how secure and efficient communication can be implemented in public safety agencies and emergency services (BOS), hospital networks, or public administration systems.

02 Share the guide internally: Use this guide as a basis for discussion within your organization. IT departments, data protection officers, compliance managers, and executives will particularly benefit from a well-rounded overview of the technical, legal, and strategic aspects of digital sovereignty.

03 From knowledge to action: Building sovereign structures requires foresight, but not radical measures overnight. The first step is often to switch particularly sensitive areas like messaging, internal communication, or personal data processing to sovereign European solutions.

About Teamwire

Company profile

Teamwire is a messaging platform, developed and operated in Germany, specifically designed for professional users in government agencies, public safety organizations, critical infrastructures, and healthcare. The company was founded with the goal of creating a true, data-sovereign alternative to consumer-oriented messaging services, with a clear focus on security, data privacy, and user-friendliness.

Mission and values

Teamwire's mission is to make digital communication secure, GDPR-compliant, and sovereign –without compromising on user experience and functionality. At its core are European values: privacy protection, legal clarity, technological transparency, and the promotion of innovation in line with democratic principles.

Location and infrastructure

Teamwire is headquartered in Munich, Germany, and operates its services exclusively in European data centers according to the highest security standards. Hosting options include cloud, private cloud, and on-premises solutions – BSI-C5 and ISO 27001 certified, fully independent of non-European law.

Imprint and legal notices

Publisher
Teamwire GmbH
Tittmoninger Straße 11
81679 Munich

Website
teamwire.eu

E-mail
info@teamwire.eu

Management
Tobias Stepan
Court of Registration: Munich District Court
HRB 187102

Concept
Tobias Strauß-Mirwald &
Stephanie Strohmeier,
Teamwire GmbH,
www.teamwire.eu,
Colorful Chairs GmbH,
www.colorfulchairs.de

Text
Colorful Chairs GmbH,
www.colorfulchairs.de,
Teamwire GmbH,
www.teamwire.eu

Layout & Grafik
Teamwire GmbH,
teamwire.eu
Colorful Chairs GmbH,
www.colorfulchairs.de

Legal Notice
The content of this whitepaper has been created with the utmost care. However, we cannot guarantee the accuracy, completeness, or current relevance of the information.